POLITYKA BEZPIECZEŃSTWA PRZETWARZANIA DANYCH OSOBOWYCH PRZEZ EURO-TAX.PL ZWROT PODATKU S.A.

I. PODSTAWA PRAWNA

1. Niniejsza „Polityka bezpieczeństwa" stanowi na dzień jej wprowadzenia wykonanie obowiązku, o którym mowa w § 4 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. z 2004 r. Nr 100, poz. 1024).
2. Jednocześnie począwszy od dnia 25 maja 2018 r. podstawę prawną dla wprowadzenia niniejszej „Polityki bezpieczeństwa" stanowi ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (dalej zwane RODO, a tu w szczególności Art. 24 ust. 2 RODO.

II. CEL OPRACOWANIA DOKUMENTU

Celem opracowania niniejszego dokumentu jest wytyczenie zasad i wymagań w zakresie ochrony danych osobowych gromadzonych i przetwarzanych przez EURO-TAX.PL ZWROT PODATKU SA, biorąc pod uwagę, że w jednostce organizacyjnej został powołany Administrator bezpieczeństwa informacji, który z chwilą wejścia w życie RODO zyskuje status Inspektora Ochrony Danych, o którym mowa w Art. 37 RODO. Ponadto, celem niniejszej Polityki Bezpieczeństwa jest ochrona danych osobowych, przetwarzanych przez EURO-TAX.PL ZWROT PODATKU SA , w szczególności ich ochrona przed udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem przepisów określających zasady postępowania przy przetwarzaniu danych osobowych oraz przed zmianą, uszkodzeniem lub zniszczeniem. Wypracowane zasady i wymagania mają ukierunkować działania zmierzające do budowy systemu bezpieczeństwa, a potem jego utrzymywania podczas eksploatacji, na poziomie odpowiadającym potrzebom organizacji.

III. CEL POLITYKI BEZPIECZEŃSTWA

Rozumiejąc konieczność zapewnienia zabezpieczenia danych osobowych przetwarzanych przez spółkę EURO-TAX.PL ZWROT PODATKU Spółka Akcyjna, w szczególności tych przetwarzanych w systemie informatycznym, która to konieczność wynika z obowiązujących przepisów prawa, jak również z zabezpieczenia interesów EURO-TAX.PL ZWROT PODATKU SA i jej klientów, Spółka deklaruje pełne wsparcie dla podejmowanych działań uzasadnionych realizacją celów zabezpieczenia przetwarzanych danych osobowych i w tym celu wprowadza i stosuje niniejszą politykę bezpieczeństwa. Celem Polityki bezpieczeństwa jest ochrona danych osobowych, przetwarzanych przez EURO-TAX.PL ZWROT PODATKU SA, w szczególności ich ochrona przed udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną,

przetwarzaniem z naruszeniem przepisów określających zasady postępowania przy przetwarzaniu danych osobowych oraz przed zmianą, uszkodzeniem lub zniszczeniem.

IV. DEFINICJE:

1) Administrator Bezpieczeństwa Informacji – osoba powołana przez administratora danych na podstawie art. 36a ust. 1 ustawy, realizująca zadania przewidziane w ustawie oraz inne obowiązki powierzone przez administratora danych, przy czym z dniem wejścia w życie RODO Administrator Bezpieczeństwa Informacji zyskuje status Inspektora Ochrony Danych w rozumieniu Art. 37 RODO;
2) Administrator danych –osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych, przy czym administratorem danych w rozumieniu niniejszej Polityki bezpieczeństwa jest EURO-TAX.PL ZWROT PODATKU SA z siedzibą: ul. Sikorskiego 2-8, Wrocław, wpisana do rejestru przedsiębiorców Krajowego Rejestru sądowego pod numerem KRS: 0000480703, REGON: 142746896, NIP: 1080009959, dalej (EURO-TAX.PL ZWROT PODATKU SA)
3) Podmiot przetwarzający - osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza dane osobowe w imieniu administratora;
4) Dane osobowe – informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to 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;
5) Dane biometryczne - 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;
6) Dane dotyczące zdrowia - dane osobowe o zdrowiu fizycznym lub psychicznym osoby fizycznej – w tym o korzystaniu z usług opieki zdrowotnej – ujawniające informacje o stanie jej zdrowia;
7) Zbiór danych - oznacza uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie;
8) Przetwarzanie danych osobowych – 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;
9) Transgraniczne przetwarzanie - przetwarzanie danych osobowych, które odbywa się w Unii w ramach działalności jednostek organizacyjnych w więcej, niż jednym państwie członkowskim administratora lub podmiotu przetwarzającego w Unii posiadającego jednostki organizacyjne w więcej niż jednym państwie

członkowskim, lub które znacznie wpływa lub może znacznie wpłynąć na osoby, których dane dotyczą, w więcej niż jednym państwie członkowskim;

10) Profilowanie - oznacza dowolną formę zautomatyzowanego przetwarzania danych osobowych, które 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;
11) Ograniczenie przetwarzania - oznaczenie przechowywanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania;
12) Pseudonimizacja - oznacza przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej;
13) Usuwanie danych – zniszczenie danych osobowych lub taka ich modyfikacja, która nie pozwala na ustalenie tożsamości osoby, której dane dotyczą ("anonimizacja"),
14) Zgoda osoby, której dane dotyczą - 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;
15) Naruszenie ochrony danych osobowych - 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;
16) Informatyczne nośniki danych – materiały lub urządzenia służące do zapisywania, przechowywania i odczytywania danych osobowych w postaci cyfrowej lub analogowej,
17) Rozliczalność danych – właściwość zapewniająca, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi,
18) Integralność danych – właściwość zapewniająca, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany,
19) Poufność danych – właściwość zapewniająca, że dane nie są udostępniane nieupoważnionym podmiotom,
20) Strona trzecia – oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub podmiot inny niż osoba, której dane dotyczą, administrator, podmiot przetwarzający czy osoby, które – z upoważnienia administratora lub podmiotu przetwarzającego – mogą przetwarzać dane osobowe
21) Główna jednostka organizacyjna oznacza: a) jeżeli chodzi o administratora posiadającego jednostki organizacyjne w więcej niż jednym państwie członkowskim – miejsce, w którym znajduje się jego centralna administracja w Unii,
22) Grupa przedsiębiorstw oznacza przedsiębiorstwo sprawujące kontrolę oraz przedsiębiorstwa przez nie kontrolowane;
23) Państwo trzecie - państwo nienależące do Europejskiego Obszaru Gospodarczego.
24) Przedsiębiorca - osoba fizyczna lub prawna prowadząca działalność gospodarczą, niezależnie od formy prawnej, w tym spółki osobowe lub zrzeszenia prowadzące regularną działalność gospodarczą;

25) RODO - ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).
26) Ustawa – ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz. U. z 2016 r., poz. 922),
27) 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. z 2004 r. Nr 100, poz. 1024),
28) Organ nadzorczy - niezależny organ publiczny ustanowiony przez państwo członkowskie UE odpowiedzialny za monitorowanie stosowania przepisów prawa o ochronie danych osobowych, w celu ochrony podstawowych praw i wolności osób fizycznych w związku z przetwarzaniem oraz ułatwiania swobodnego przepływu danych osobowych w UE, przy czym na dzień wprowadzenia niniejszej Polityki bezpieczeństwa organem nadzorczym wyznaczonym przez Rzeczpospolitą Polską jest Generalny Inspektor Ochrony Danych Osobowych.

V. ZASADY OGÓLNE PRZETWARZANIA DANYCH

1. Przetwarzane danych osobowych w systemie EURO-TAX.PL ZWROT PODATKU S.A. realizowane jest zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą („zgodność z prawem, rzetelność i przejrzystość"), z zachowaniem zasad ograniczenia celu i zakresu przetwarzania, minimalizacji danych, adekwatności i prawidłowości, poufności i rozliczalności ich przetwarzania.
2. Przetwarzanie danych osobowych o szczególnym charakterze, w szczególności: ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz przetwarzania danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej lub danych dotyczących zdrowia, seksualności lub orientacji seksualnej tej osoby, może nastąpić wyłącznie na podstawie wyraźnych upoważnień zawartych w przepisach prawa i z nich wynikających.
3. W ramach zabezpieczenia danych osobowych ochronie na zasadach określonych w niniejszej Polityce bezpieczeństwa podlegają:
   a) sprzęt komputerowy – serwer, komputery osobiste (w tym laptopy) i inne urządzenia zewnętrzne,
   b) oprogramowanie,
   c) dane osobowe zapisane na informatycznych nośnikach danych oraz dane przetwarzane w systemach informatycznych,
   d) hasła użytkowników,
   e) bazy danych i kopie zapasowe,
   f) wydruki,
   g) związana z przetwarzaniem danych dokumentacja papierowa.
4. Zabezpieczenie danych osobowych obejmuje:
   a) ochronę poufności rozumianej jako zabezpieczenie informacji przed dostępem do niej osób nieuprawnionych,

b) ochronę integralności rozumianej jako zabezpieczenie informacji przed wprowadzeniem przypadkowych lub celowych zmian powodujących jej zafałszowanie,
c) ochronę dostępności rozumianej jako zabezpieczenie informacji przed jej zniszczeniem, jak również zapewnienie takiego działania systemu informatycznego, aby dane osobowe były dostępne dla osób upoważnionych do dostępu do nich, a także do ich przetwarzania

5. Wszystkie osoby biorące bezpośredni lub pośredni udział w procesie przetwarzania danych osobowych w szczególności przetwarzanych w systemie informatycznym są odpowiedzialne za właściwe zabezpieczenie tych danych.
6. Zabezpieczenia są określone na podstawie obowiązujących wymagań prawnych i wyników analizy ryzyka. Za koordynację procesu analizy ryzyka odpowiedzialny jest Administrator Bezpieczeństwa informacji/ Inspektor Ochrony Danych.
7. Przetwarzanie danych osobowych w systemach informatycznych jest dopuszczalne pod warunkiem:
   a) zdolności systemu do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania;
   b) zdolności systemu do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego;
   c) regularnego testowania, mierzenia i oceniania skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania;
   d) spełnienia szczegółowych zaleceń dotyczących systemów informatycznych opisanych w niniejszej polityce bezpieczeństwa, jak również w dokumentach z nią związanych,
   e) posiadania przez systemy informatyczne mechanizmów pozwalających na realizację procesów zabezpieczenia danych osobowych opisanych w niniejszej polityce, jak również w dokumentach z nią związanych;
   f) przetwarzania danych osobowych w zakresie dopuszczalnym ze względu na przepisy prawa o ochronie danych osobowych.
8. Szczegółowe zasady zarządzania systemem informatycznym służącym do przetwarzania danych osobowych EURO-TAX.PL ZWROT PODATKU S.A. zawiera Załącznik nr 5 do Polityki bezpieczeństwa EURO-TAX.PL ZWROT PODATKU S.A. „INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH EURO-TAX.PL ZWROT PODATKU S.A."

VI. OBSZAR PRZETWARZANIA DANYCH OSOBOWYCH

1. Przetwarzanie danych osobowych przez EURO-TAX.PL ZWROT PODATKU SA odbywa się zarówno przy wykorzystaniu systemów informatycznych jak i poza nimi, tj. w wersji tradycyjnej, „papierowej".
2. Systemy informatyczne przetwarzające dane osobowe umieszczane są w wydzielonych pomieszczeniach, do których dostęp jest kontrolowany. Pracownicy upoważnieni do dostępu do pomieszczeń są zobowiązani do nie wpuszczania osób nieposiadających zgody członka zarządu, pełnomocnika administratora danych osobowych ds. Zarządzania uprawnieniami lub Administratora Bezpieczeństwa Informacji/Inspektora Ochrony Danych. Szczegółowe zasady zarządzania uprawnieniami do przetwarzania danych zawiera Załącznik nr 6 „INSTRUKCJA ZARZĄDZANIA UPRAWNIENIAMI DO KORZYSTANIA Z SYSTEMU INFORMATYCZNEGO".

3. Obszar przetwarzania danych osobowych przez EURO-TAX.PL ZWROT PODATKU SA został określony w Załączniku nr 1 do Polityki bezpieczeństwa pt.: „Wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w których przetwarzane są dane osobowe". Za obszar przetwarzania danych należy rozumieć obszar, w którym wykonywana jest choćby jedna z czynności przetwarzania danych osobowych.
4. Dane osobowe są i mogą być przetwarzane wyłącznie w miejscach wskazanych w załączniku nr 1 i przy zastosowaniu środków ochrony wskazanych w punkcie VII i załączniku nr 1.
5. Dane osobowe mogą być przetwarzane na komputerach znajdujących się poza wyznaczoną strefą lub pomieszczeniem pod warunkiem zastosowania szczególnych warunków bezpieczeństwa określonych dla tego rodzaju urządzeń. W szczególności zasady przetwarzania danych na komputerach przenośnych określa ZAŁĄCZNIK nr 7 do niniejszej Polityki bezpieczeństwa - „INSTRUKCJA KORZYSTANIA Z KOMPUTERÓW PRZENOSNYCH PRZETWARZAJACYCH DANE OSOBOWE".

VII. ZBIORY DANYCH EURO-TAX.PL ZWROT PODATKU SA I ICH STRUKTURA

Opis struktury zbiorów danych EURO-TAX.PL ZWROT PODATKU SA, i wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania danych, wskazujący zawartość poszczególnych pól informacyjnych i powiązania pomiędzy nimi, a także sposób przepływu danych pomiędzy poszczególnymi systemami, przedstawia Załącznik nr 2 do niniejszej Polityki bezpieczeństwa.

VIII. ZASADY PRZEKAZYWANIA DANYCH I ICH PRZEPŁYWU MIĘDZY SYSTEMAMI

1. Dane osobowe przekazywane są pomiędzy systemami i modułami w sposób wskazany w Załączniku nr 2 do niniejszej Polityki bezpieczeństwa. Przekazywanie danych w celu ich przetwarzania podmiotom innym niż administrator jest objęte odrębną umową o powierzeniu przetwarzania danych osobowych.
2. Przekazywanie danych osobowych do innych podmiotów z Grupy Kapitałowej EURO-TAX.PL ZWROT PODATKU S.A. przez EURO-TAX.PL ZWROT PODATKU S.A. odbywa się drogą elektroniczną i ustalone jest odrębnymi umowami o powierzeniu przetwarzania danych osobowych zawieranymi z każdym podmiotem.
3. Przekazanie danych osobowych do państwa trzeciego lub organizacji międzynarodowej może nastąpić bez specjalnego zezwolenia, wyłącznie gdy Komisja Europejska stwierdzi, że to państwo trzecie, terytorium lub określony sektor lub określone sektory w tym państwie trzecim lub dana organizacja międzynarodowa zapewniają odpowiedni stopień ochrony, lub w razie nie dokonania przez Komisję Europejską takiej kwalifikacji, wyłącznie, gdy zapewnią one odpowiednie zabezpieczenia, i pod warunkiem, że obowiązują egzekwowalne prawa osób, których dane dotyczą, i skuteczne środki ochrony prawnej. W innym przypadku przekazanie wymaga specjalnego zezwolenia.
4. Wymiana danych osobowych pomiędzy użytkownikami systemu informatycznego dozwolona jest tylko zgodnie z zasadami przepływu danych osobowych. Pracami zespołu kieruje Administrator Bezpieczeństwa Informacji/Inspektor Ochrony Danych.
5. Przekazywanie danych zgromadzonych w zbiorach prowadzonych w formie papierowej/ drukowanej odbywa się to tylko w formie papierowej, przekazywanie następuje osobiście między osobami z obu stron do tego upoważnionymi.
6. Dostęp użytkowników do systemu informatycznego przetwarzającego dane osobowe jest kontrolowany za

pomocą mechanizmów uwierzytelniania, autoryzacji i rozliczalności. Podstawą uwierzytelniania użytkownika jest unikalny dla użytkownika identyfikator i hasło. Hasło nie może być przekazane przez użytkownika jakiejkolwiek innej osobie, jedynym wyjątkiem jest przekazywanie przez administratora tymczasowego hasła użytkownikowi. Autoryzacja użytkownika odbywa się na podstawie Identyfikatora i hasła. System informatyczny przetwarzający dane osobowe jest wyposażony w mechanizmy pozwalające w sposób jednoznaczny przypisać wykonanie określonych operacji na danych osobowych konkretnemu użytkownikowi. Rodzaje operacji i szczegółowość zapisu jest określana w oparciu o wyniki analizy ryzyka oraz obowiązujące regulacje prawne.

IX. FORMA LUB OPROGRAMOWANIE WYKORZYSTYWANE PRZY PRZETWARZANIU DANYCH

Opis oprogramowania używanego do przetwarzania poszczególnych elementów struktury zbiorów danych EURO-TAX.PL ZWROT PODATKU S.A. zawarty jest w Załączniku nr 2 do niniejszej Polityki bezpieczeństwa.

X. ŚRODKI OCHRONY I ZABEZPIECZENIA DANYCH

1. Wprowadza się elementy zabezpieczenia danych osobowych przez EURO-TAX.PL ZWROT PODATKU S.A.:
   - **a)** stosowane metody ochrony pomieszczeń, w których przetwarzane są dane osobowe (zabezpieczenia fizyczne), w tym w szczególności:
     - i) wydzielenie obszaru przetwarzania danych,
     - ii) dostęp do pomieszczeń, w których przetwarzane są dane osobowe objęty jest systemem kontroli dostępu,
     - iii) samodzielny dostęp do pomieszczeń jest możliwy wyłącznie dla osób upoważnionych, wstęp osób postronnych jest możliwy jedynie podczas obecności pracowników Kancelarii,
     - iv) przechowywanie akt w wersji papierowej w specjalnie do tego celu przeznaczonych pomieszczeniach, w zamykanych na klucz szafach,
     - v) kopie zapasowe zbioru danych osobowych przechowywane są w sejfie w innym pomieszczeniu niż to, w którym znajduje się serwer, na którym dane osobowe przetwarzane są na bieżąco,

   - b) odpowiednie środki zabezpieczenia danych w systemach informatycznych (zabezpieczenia techniczne), w tym w szczególności:
     - i. systemy informatyczne zastosowane do przetwarzania danych osobowych spełniają wymagania określone w przepisach prawa na poziomie wysokim,
     - ii. zastosowano mechanizmy kontroli dostępu do systemów informatycznych i ich zasobów; zróżnicowane dla różnych grup użytkowników,
     - iii. zastosowano odpowiednie i regularnie aktualizowane narzędzia ochronne, w tym oprogramowanie antywirusowe,
     - iv. system informatyczny służący do przetwarzania danych osobowych chroni się przed zagrożeniami pochodzącymi z sieci publicznej poprzez wdrożenie fizycznych i logicznych zabezpieczeń chroniących przed nieuprawnionym dostępem,
     - v. tworzone są regularnie kopie zapasowe zbiorów danych przetwarzanych w systemach informatycznych oraz kopie programów służących do przetwarzania danych osobowych,

vi. zastosowano zabezpieczenia systemu przed utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej (listwy przeciwzakłóceniowe),

vii. systemy informatyczne i zbiory danych w nich przetwarzane projektowane są i wdrażane w sposób zapewniający możliwość przetwarzania danych z zachowaniem zasady, dostępności, zupełności, poufności, integralności i rozliczalności ochrony danych i innych zasad przyjętych w niniejszej Polityce bezpieczeństwa .

c) zabezpieczenia organizacyjne i osobowe, w tym w szczególności:

i. powołano Administratora Bezpieczeństwa Informacji/Inspektora Ochrony Danych nad wprowadzonymi zasadami i procedurami zabezpieczenia danych;

ii. przetwarzanie danych osobowych może być wykonywane wyłącznie przez osoby, które zostały upoważnione do przetwarzania danych osobowych poprzez wpisanie określonych kompetencji do zakresu obowiązków na danym stanowisku do ewidencji stanowiącej załącznik 4 do Polityki bezpieczeństwa i które zobowiązane są do utrzymywania w tajemnicy danych osobowych i sposobów ich zabezpieczenia, również po odwołaniu z określonego stanowiska, a także po ustaniu zatrudnienia; w tym celu osoby te podpisują oświadczenie o utrzymywaniu w tajemnicy danych osobowych i sposobów ich zabezpieczenia, szczegółowe zasady przetwarzania danych osobowych osób fizycznych określa ZAŁĄCZNIK NR 8 – „INSTRUKCJA W SPRAWIE PRZETWARZANIA DANYCH OSOBOWYCH OSÓB FIZYCZNYCH I ZAPEWNIENIA WYKONANA UPRAWNIEŃ PRZYSŁUGUJĄCYCH TYM OSOBOM"

iii. zapewniono bieżącą kontroluję pracy systemu informatycznego z obowiązkiem niezwłocznego informowania o zaobserwowanych nieprawidłowościach Administratora Bezpieczeństwa Informacji/Inspektora Ochrony Danych;

d) środki ochrony w ramach oprogramowania urządzeń teletransmisji, w szczególności:

i. dostęp do urządzeń teletransmisyjnych realizowany jest z wykorzystaniem dedykowanej, separowanej strefy komunikacyjnej z wykorzystaniem protokołów szyfrujących przesyłane dane. Każdy administrator i użytkownik, posiada własne konto, chronione, tylko jemu znanym hasłem lub kryptograficznym kluczem prywatnym.

ii. środki ochrony w ramach oprogramowania systemów:
   – szyfrowanie transmisji danych osobowych pomiędzy użytkownikiem, a serwerem WWW wg standardu SSL/TLS.
   – uwierzytelnienie użytkowników za pomocą systemu haseł
   – kontrolowany dostęp do systemu operacyjnego i aplikacji,

iii. środki ochrony w ramach narzędzi baz danych i innych narzędzi programowych:
   – zdalny dostęp do serwera bazy danych jedynie z adresu serwera WWW,
   – system dostępu do baz danych przy pomocy loginów i haseł,.

e) zabezpieczenie nośników, w szczególności:

i. wszelkiego rodzaju nośniki danych osobowych, które są przekazywane osobom lub podmiotom nieupoważnionym do otrzymania tych danych, lub też gdy istnieje podejrzenie, że mogą się one znaleźć w rekach osób nieupoważnionych do otrzymania danych osobowych, pozbawia się danych lub też doprowadza do stanu uniemożliwiającego ich odczytanie. Za pozbawienie zapisu odpowiada osoba przekazująca nośnik lub odpowiadająca za realizację działań, w których wyniku nośnik może stać się dostępny dla osób nieupoważnionych do otrzymania danych osobowych.

ii. w razie gdy przekazanie nośnika jest związane z jego naprawą lub konserwacją albo naprawą lub konserwacją urządzenia, którego składową jest nośnik, dopuszczalne jest pozostawienie zapisanych danych pod warunkiem sprawowania nadzoru przez upoważnionego administratora bezpieczeństwa informacji pracownika EURO-TAX.PL ZWROT PODATKU S.A. podczas prowadzenia naprawy lub konserwacji.

iii. dane osobowe są zabezpieczane przez tworzenie kopii awaryjnych. Za poprawność przebiegu procesu tworzenia kopii awaryjnych, jak również za bezpieczne składowanie nośników kopii i ich udostępnianie odpowiada Administrator Bezpieczeństwa Informacji/Inspektor Ochrony Danych. Za składowanie informacji w sposób umożliwiający wykonanie kopii, w szczególności na centralnych serwerach, odpowiadają użytkownicy systemu informatycznego.

iv. wszelkiego rodzaju nośniki danych osobowych, w tym również kopie zapasowe danych osobowych przechowywane są w sposób zapewniający odpowiednią ochronę przed dostępem do nich osób niepowołanych oraz przed celowym lub przypadkowym zniszczeniem, w tym również zniszczeniem wynikającym z warunków środowiskowych.

v. realizacja w/w wytycznych, za którą odpowiedzialność ponosi Administrator Bezpieczeństwa Informacji/Inspektor Ochrony Danych polega na:

- ich przechowywaniu w wydzielonym pomieszczeniu specjalnie do tego przeznaczonym w pomieszczeniach wymienionych w Załączniku nr 1 do niniejszej Polityki bezpieczeństwa
- pomieszczenia te są zamykane na klucz, który jest przechowywany w ..., odpowiedzialną osobą za dostęp do Archiwum jest Asystentka Zarządu
- Klucze do Archiwum są udostępniane jedynie Zarządowi Spółki, w razie nieobecności osoby odpowiedzialnej za archiwum odpowiedzialna jest osoba zastępująca ....
- Przy każdorazowym pobraniu kluczy do Archiwum zostaje to odnotowane w ewidencji wydawania klucza do Archiwum.

XI. ADMINISTRATOR BEZPIECZEŃSTWA INFORMACJI /INSPEKTOR OCHRONY DANYCH.

1. Zarząd EURO-TAX.PL ZWROT PODATKU SA wyznacza Administratora Bezpieczeństwa Informacji/Inspektora Ochrony Danych w celu sprawowania nadzoru nad przestrzeganiem obowiązujących zasad bezpieczeństwa danych osobowych, w tym w szczególności koordynacji procesów związanych z zarządzaniem systemem informatycznym przetwarzającym dane osobowe w aspekcie ich bezpieczeństwa oraz reprezentowania administratora danych osobowych w obszarach bezpośrednio wskazanych przez zarząd Spółki.
2. Administrator Bezpieczeństwa Informacji/Inspektor Ochrony Danych wypełnia swoje zadania z należytym uwzględnieniem ryzyka związanego z operacjami przetwarzania, mając na uwadze charakter, zakres, kontekst i cele przetwarzania.

3. Do kompetencji Administratora Bezpieczeństwa Informacji/Inspektora Ochrony Danych należy:

a) monitorowanie i sprawdzanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz powiązane z tym audyty;

b) nadzorowanie opracowania i aktualizowania dokumentacji opisującej sposób przetwarzania danych oraz środki techniczne i organizacyjne oraz przestrzeganie zasad określonych w dokumentacji;

c) zapewnianie zapoznawania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych, w tym ustalanie podziału obowiązków, planowanie działań zwiększających świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania;

d) prowadzenie rejestru zbiorów danych przetwarzanych przez administratora danych;

e) współpraca z organem nadzorczym i pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach.

4. Do obowiązków Administratora Bezpieczeństwa Informacji/Inspektora Ochrony Danych należy:

a) informowanie administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy przepisów prawa o ochronie danych i doradzanie im w tej sprawie;

b) udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania;

c) nadzór na opracowaniem i aktualizacją dokumentacji opisującej zastosowaną ochronę danych osobowych (niniejsza Polityka oraz wynikające z niej instrukcje i procedury) oraz zapewnienie ich publikacji i dystrybucji i przestrzeganie zasad w nich określonych, poprzez:

   i) weryfikowanie opracowania i kompletności dokumentacji;

   ii) weryfikowanie zgodności dokumentacji z obowiązującymi przepisami prawa;

   iii) weryfikowanie stanu faktycznego w zakresie przetwarzania danych osobowych;

   iv) weryfikowanie zgodności ze stanem faktycznym przewidzianych w dokumentacji środków technicznych i organizacyjnych służących przeciwdziałaniu zagrożeniom dla ochrony danych osobowych.

d) uzgadnianie z osobami odpowiedzianymi za obsługę systemów informatycznych szczególnych procedur regulujących wykonywanie czynności w systemach lub aplikacjach służących do przetwarzania danych osobowych,

e) nadzór nad wdrożeniem, przestrzeganiem i stosowaniem i stosownych środków organizacyjnych, technicznych i fizycznych oraz systemu procedur bezpieczeństwa w celu ochrony przetwarzanych danych osobowych;

f) nadawanie, zmienianie oraz cofanie uprawnień do przetwarzania danych osobowych oraz prowadzenie ewidencji użytkowników systemów informatycznych, w których przetwarzane są dane osobowe, stanowiącej część ewidencji osób upoważnionych do przetwarzania danych osobowych oraz wszelkiej dokumentacji opisującej sposób realizacji i stopień ochrony danych osobowych w EURO-TAX.PL ZWROT PODATKU S.A. a także kontrolowanie nadanych w systemach informatycznych uprawnień do przetwarzania danych osobowych pod kątem ich zgodności z wpisami umieszczonymi w ewidencji osób upoważnionych do przetwarzania danych osobowych;

g) zapoznawanie pracowników oraz współpracowników EURO-TAX.PL ZWROT PODATKU S.A. z

przepisami i zasadami ochrony danych osobowych oraz informowanie o zagrożeniach związanych z ich przetwarzaniem, w tym prowadzenie szkoleń dla osób upoważnionych w zakresie przepisów o ochronie danych osobowych w szczególności dla użytkowników w zakresie stosowanych w systemach informatycznych środków ochrony danych osobowych;

h) przygotowywanie zgłoszeń zbiorów danych osobowych do rejestracji w organie nadzorczym, o ile rejestracja jest wymagana;

i) wskazywanie zagrożeń oraz reagowanie na naruszenia ochrony danych osobowych zgłaszane incydenty związane z naruszeniem ochrony danych osobowych oraz analizowanie ich przyczyn, usuwanie ich skutków i kierowanie wniosków dotyczących ukarania winnych naruszeń, a także W przypadku naruszenia ochrony danych osobowych, informowanie o naruszeniu bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia, organu nadzorczego, o ile zgodnie z obowiązującym prawem powstaje taki obowiązek informacyjny;

j) dokonywanie sprawdzeń zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych polegających na weryfikacji zbiorów danych osobowych i systemów informatycznych. Sprawdzenia są dokonywane na wniosek Zarządu EURO-TAX.PL ZWROT PODATKU S.A. Administrator Bezpieczeństwa Informacji/Inspektor Ochrony Danych może dokonać sprawdzenia także w sytuacji powzięcia wiadomości o naruszeniu ochrony danych osobowych lub uzasadnionego podejrzenia wystąpienia takiego naruszenia;

k) dokumentowanie czynności przeprowadzonych w toku sprawdzenia, w zakresie niezbędnym do oceny zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych. Dokumentowanie czynności w toku sprawdzenia może polegać, w szczególności, na utrwaleniu danych z systemu informatycznego służącego do przetwarzania lub zabezpieczania danych osobowych na informatycznym nośniku danych lub dokonaniu wydruku tych danych oraz w szczególności na:
   i) sporządzeniu notatki z czynności, w szczególności z zebranych wyjaśnień, przeprowadzonych oględzin oraz z czynności związanych z dostępem do urządzeń, nośników oraz systemów informatycznych;
   ii) odebraniu wyjaśnień osoby, której czynności objęto sprawdzeniem;
   iii) sporządzeniu kopii otrzymanego dokumentu;
   iv) sporządzeniu kopii obrazu wyświetlonego na ekranie urządzenia stanowiącego część systemu informatycznego lub zabezpieczania danych osobowych;
   v) sporządzeniu kopii zapisów rejestrów systemu informatycznego lub zapisów konfiguracji technicznych środków zabezpieczeń tego systemu;

l) w przypadkach wykrycia rażących zaniedbań w toku sprawdzenia sporządzenie ich opisu i niezwłoczne przedłożenie administratorowi danych stosownego sprawozdania;

m) prowadzenie rejestrów czynności przetwarzania danych, o ile administrator objęty jest obowiązkiem ich prowadzenia;

n) wykonywanie innych czynności w celu zapewnienia przepisów o ochronie danych osobowych w EURO-TAX.PL ZWROT PODATKU S.A..

XII. INCYDENTY ZWIĄZANE Z ZAGROŻENIEM I NARUSZENIEM OCHRONY DANYCH OSOBOWYCH

1. W wypadku wystąpienia przypadkowego lub celowego naruszenia bezpieczeństwa danych osobowych Administrator Bezpieczeństwa Informacji/Inspektor Ochrony Danych jest odpowiedzialny za przeprowadzenie procesu usuwania skutków naruszenia bezpieczeństwa danych osobowych z uwzględnieniem wykrycia przyczyn zaistnienia incydentu, przekazania zarządowi spółki o ewentualnych sprawcach oraz przeanalizowania możliwości wprowadzenia zabezpieczeń redukujących ryzyko wystąpienia w przyszłości podobnego incydentu.
2. Każda osoba która zauważy naruszenie bezpieczeństwa danych osobowych, a w szczególności:
   a) ujawnienie lub możliwość ujawnienia danych osobowych osobom nieupoważnionym,
   b) zafałszowanie danych osobowych lub możliwość wystąpienia zafałszowania danych osobowych,
   c) zniszczenie lub możliwość zablokowania pracy systemu informatycznego przetwarzającego dane osobowe

   zobowiązana jest natychmiast powiadomić administratora bezpieczeństwa informacji lub osoby przez niego upoważnione.
3. Naruszenie bezpieczeństwa danych osobowych przetwarzanych w systemie informatycznym w szczególności obejmuje wprowadzenie do systemu wirusów lub innych wrogich kodów, jak również dostęp do systemu informatycznego osób niepowołanych (fizyczny- poprzez bezpośredni dostęp do komputera, na którym przetwarzane są dane osobowe, oraz logiczny- poprzez dostęp do danych osobowych za pośrednictwem sieci informatycznych). Szczegółowe zasady reagowania na incydenty związane z naruszeniem bezpieczeństwa danych osobowych zawiera załącznik nr 9 - „INSTRUKCJA POSTĘPOWANIA W PRZYPADKU WYSTĄPIENIA INCYDENTU LUB NARUSZENIA OCHRONY DANYCH OSOBOWYCH", za której przygotowanie i uaktualnianie odpowiada administrator bezpieczeństwa informacji.
4. Administrator Bezpieczeństwa Informacji/Inspektor Ochrony Danych, jako podmiot odpowiedzialny za prowadzenie działań mających na celu zabezpieczenie systemu informatycznego przetwarzającego dane osobowe przed zainfekowaniem wirusami lub innymi niebezpiecznymi kodami, ma prawo ograniczać uprawnienia użytkowników, w szczególności w zakresie wymiany informacji z wykorzystaniem publicznych sieci informatycznych, jeżeli może to wpłynąć na redukcję ryzyka wprowadzenia wirusów lub innych wrogich kodów do systemu informatycznego przetwarzającego dane osobowe i nie będzie miało wpływu na możliwość realizacji przez pracowników Spółki ich obowiązków służbowych.
5. Pracownicy EURO-TAX.PL ZWROT PODATKU S.A. korzystający z systemu informatycznego są zobowiązani do stosowania się do szczegółowych zaleceń w zakresie ochrony antywirusowej, a także do przedmiotowych zaleceń wydawanych przez administratora bezpieczeństwa informacji.
6. Administrator, a tu z jego upoważnienia Administrator Bezpieczeństwa Informacji/Inspektor Ochrony Danych, informuje o naruszeniu organ nadzorczy bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia, o ile zgodnie z obowiązującym prawem powstaje taki obowiązek informacyjny, przy czym zgłoszenie takie musi co najmniej:
   a) opisywać charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazywać kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;
   b) zawierać imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego

punktu kontaktowego, od którego można uzyskać więcej informacji;

c) opisywać możliwe konsekwencje naruszenia ochrony danych osobowych;

d) opisywać środki zastosowane lub proponowane przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

7. Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, Administrator, a tu z jego upoważnienia Administrator Bezpieczeństwa Informacji/Inspektor Ochrony Danych, bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu.
8. W celu usprawnienia działań podejmowanych w ramach zabezpieczenia danych przed incydentami i naruszeniami ochrony danych, Administrator Bezpieczeństwa Informacji/Inspektor Ochrony Danych może powołać specjalny zespół reagowania na incydenty i naruszenia.
9. Szczegółowe zasady postępowania w razie incydentu lub naruszenia ochrony danych zawarte są w „Instrukcji Postępowania W Przypadku Wystąpienia Incydentu Lub Naruszenia Ochrony Danych Osobowych" stanowiąca załącznik nr

XIII. ZAKRES I OBOWIĄZEK STOSOWANIA POLITYKI BEZPIECZEŃSTWA

1. Wszyscy pracownicy EURO-TAX.PL ZWROT PODATKU S.A. mający dostęp do danych osobowych w szczególności przetwarzanych w ramach systemu informatycznego są poddawani przeszkoleniu obejmującemu zapoznanie z obowiązującymi regulacjami prawnymi w zakresie ochrony danych osobowych, jak również obowiązującymi w EURO-TAX.PL ZWROT PODATKU S.A. zasadami bezpiecznego ich przetwarzania. Za przeprowadzenie szkolenia odpowiada administrator bezpieczeństwa informacji, za organizację szkolenia odpowiada przełożony szkolonych pracowników. Przeszkolenie pracownika jest warunkiem koniecznym do korzystania z systemu informatycznego przetwarzającego dane osobowe.
2. Niniejsza polityka bezpieczeństwa obowiązuje wszystkich pracowników i zleceniobiorców EURO-TAX.PL ZWROT PODATKU S.A. mających dostęp do systemu informatycznego przetwarzającego dane osobowe.
3. Z uwagi na fakt, że niniejszy dokument zawiera informacje o zabezpieczeniach, dlatego też został objęty ochroną na zasadzie tajemnicy przedsiębiorstwa w myśl art. 11 ust. 4 ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (t.j. Dz. U. z 2003 r. Nr 153, poz. 1503 ze zm.). Wybrane jego elementy mogą zostać udostępnione innym podmiotom po zawarciu stosownej umowy o zachowaniu poufności.
4. Z treścią niniejszego dokumentu powinny zostać zapoznane wszystkie osoby upoważnione do przetwarzania danych osobowych, które z racji wykonywanych obowiązków i czynności mają dostęp do danych osobowych.
5. Za zarządzanie dokumentem Polityki Bezpieczeństwa, w tym jego rozpowszechnianiem, aktualizacją, utrzymywaniem spójności z innymi dokumentami, jest odpowiedzialny administrator danych.
6. Nieprzestrzeganie zasad ochrony danych osobowych zagrożone jest konsekwencjami karnymi, w szczególności na dzień wejścia w życie niniejszej Polityki, zgodnie z przepisami prawa w tym na dzień wprowadzenia niniejszej Polityki bezpieczeństwa, art.49- 54 Ustawy z dnia 29 sierpnia 1997r. O

ochronie danych osobowych.

7. Integralną część niniejszej Polityki Bezpieczeństwa stanowią następujące załączniki:
   a) Załącznik nr 1 – Wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w których przetwarzane są dane osobowe;
   b) Załącznik nr 2 – Wykaz zbiorów danych i systemów zastosowanych do ich przetwarzania;
   c) Załącznik nr 3 – Wzór upoważnienia do przetwarzania danych osobowych;
   d) Załącznik nr 4 – Ewidencja osób upoważnionych do przetwarzania danych osobowych;
   e) Załącznik nr 5 - „INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH EURO-TAX.PL ZWROT PODATKU S.A.";
   f) Załącznik nr 6 - „INSTRUKCJA ZARZĄDZANIA UPRAWNIENIAMI DO KORZYSTANIA Z SYSTEMU INFORMATYCZNEGO";
   g) ZAŁĄCZNIK nr 7 - INSTRUKCJA KORZYSTANIA Z KOMPUTERÓW PRZENOSNYCH PRZETWARZAJACYCH DANE OSOBOWE;
   h) ZAŁĄCZNIK NR 8 – „INSTRUKCJA W SPRAWIE PRZETWARZANIA DANYCH OSOBOWYCH OSÓB FIZYCZNYCH I ZAPEWNIENIA WYKONANA UPRAWNIEŃ PRZYSŁUGUJĄCYCH TYM OSOBOM";
   i) Załącznik nr 9 - INSTRUKCJA POSTĘPOWANIA W PRZYPADKU WYSTĄPIENIA INCYDENTU LUB NARUSZENIA OCHRONY DANYCH OSOBOWYCH.

XIV. Niniejsza polityka bezpieczeństwa została zatwierdzona przez zarząd EURO-TAX.PL ZWROT PODATKU S.A. dnia 14.05.2018 r.