POLITYKA BEZPIECZEŃSTWA

TADEO TRADING SP. Z O.O.

WARSZAWA 25.05.2018 r.

§ 1
Podstawa prawna i cel opracowania dokumentu

1. Niniejszy dokument został stworzony w celu wdrożenia wymogów określonych w powszechnie obowiązujących przepisach prawa, w tym nade wszystko w Rozporządzeniu 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) z dnia 27 kwietnia 2016 r.
2. Przedmiotowy akt należy odczytywać łącznie z pozostałym wewnętrznymi regulacjami takimi jak:
   a) Rejestr czynności przetwarzania danych osobowych (który to dokument określa w szczególności kategorie przetwarzanych danych, podstawę ich przetwarzania, cel, kategorie odbiorców danych);
   b) Instrukcja zarządzania system informatycznym (której celem jest wzmocnienie poziomu ochrony danych przetwarzanych w inny sposób niż w formie tradycyjnej).

§ 2
Definicje

1) **Administrator danych** – TADEO TRADING spółka z ograniczoną odpowiedzialnością, z siedzibą w Warszawie (03-684) ul Mechaników 12B, wpisana do rejestru przedsiębiorców prowadzonego przez Sąd Rejonowy dla m. st. Warszawy XIII Wydział Gospodarczy KRS: 0000015606 (dalej również jako Spółka).
2) **Dane osobowe** – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej (osoby, 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),
3) **przetwarzanie danych osobowych** – jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie udostępnianie i usuwanie, a zwłaszcza te które wykonuje się w systemach informatycznych,
4) **usuwanie danych** – zniszczenie danych osobowych
5) **anonimizacja –** modyfikacja danych, na skutek której brak jest możliwości ustalenia tożsamości osoby, której dane dotyczą,

6) **użytkownik** - rozumie się przez to upoważnionego przez Administratora danych, wyznaczonego do przetwarzania danych osobowych Pracownika;

7) **pracownik** - należy przez to rozumieć osobę zatrudnioną przez Administratora danych w formie umowy o pracę lub umowy cywilno-prawnej lub inną osobę współpracującą;

§ 3
Cel polityki bezpieczeństwa

Celem Polityki Bezpieczeństwa przetwarzania danych osobowych u Administratora jest uzyskanie optymalnego i zgodnego z wymogami obowiązujących aktów prawnych, sposobu przetwarzania informacji zawierających Dane osobowe, a przede wszystkim zapewnienie ochrony przetwarzanych Danych osobowych przed wszelkiego rodzaju zagrożeniami, tak zewnętrznymi jak i wewnętrznymi.

§ 4
Zakres stosowania Polityki Bezpieczeństwa

1. W ramach zabezpieczenia danych osobowych ochronie podlegają w szczególności:

a) sprzęt komputerowy – serwer, komputery osobiste (w tym przenośne) i inne urządzenia zewnętrzne,
b) oprogramowanie
c) Dane osobowe przetwarzane w formie tradycyjnej

2. Należy pamiętać, że Dane osobowe:

a) mogą przybrać różną formę: formularze aplikacyjne, wnioski, kwestionariusze, oświadczenia, umowy, akta osobowe, dokumentacja postępowań, ankiety, wydruki robocze, źródłowe dokumenty finansowe, orzeczenia sądów powszechnych, dokumentacja medyczna oraz wiele innych
b) dla oceny, czy określona informacja stanowi Dane osobowe czy też nie, forma nie ma decydującego znaczenia. Istotne jest to, czy informacja dotyczy osoby fizycznej oraz czy na jej podstawie możliwe jest jej zidentyfikowanie.

§ 5
Podstawowe zasady ochrony Danych osobowych

Administrator danych dąży do realizacji następujących zasad:

a) **Legalności** – przetwarzanie Danych osobowych może się odbywać wyłącznie, gdy zaistnieje co najmniej jedna z przewidzianych prawem przesłanek (przepis prawa, konieczność realizacji umowy, odrębna zgoda);

b) **Celowości** – aby dane mogły być przetwarzane, musi istnieć ku temu konkretny, wyraźny i prawnie uzasadniony cel. Jeżeli przetwarzanie służy różnym celom, potrzebna jest podstawa na wszystkie cele. Cel zbierania danych powinien być zakomunikowany osobie, której dane dotyczą;

c) **Adekwatności** – przetwarzając dane Administrator powinien kierować się zasadą minimalizacji danych – powinien on przetwarzać tylko takie dane, które są mu niezbędne ze względu na cel ich zbierania;

d) **Merytorycznej poprawności** – Administrator danych jest zobowiązany do tego, aby dane przez niego zbierane były poprawne i w razie potrzeby uaktualniane. Powinien oceniać wiarygodność źródła pozyskania danych oraz wdrożyć sposób weryfikowania prawdziwości przetwarzanych danych;

e) **Czasowości** – zasada ograniczenia przechowywania danych – obowiązek przechowywania danych osobowych przez okres nie dłuższy niż jest niezbędne do celów, w których dane te są przetwarzane;

f) **Integralności i poufności danych** – forma przetwarzania danych osobowych powinna być tak zabezpieczona za pomocą odpowiednich środków technicznych lub organizacyjnych, by zapewniała adekwatne bezpieczeństwo danych osobowych, w tym ochronę przed niezgodnym z prawem przetwarzaniem, przypadkową utratą, zniszczeniem lub uszkodzeniem;

g) **Rozliczalności –** administrator danych powinien móc wykazać, iż postępuje zgodnie z zasadami dotyczącymi przetwarzania danych osobowych;

h) **Przejrzystości** – informacje kierowane do osoby, której dane dotyczą, związane z przetwarzaniem jej danych, mają być dla niej łatwo dostępne,

zrozumiałe, oraz sformułowane jasnym i prostym językiem. Osobom fizycznym należy uświadomić ryzyka, zasady, zabezpieczenia i prawa związane z przetwarzaniem danych osobowych oraz sposoby ich wykonywania.

§ 6
Obszar przetwarzania danych osobowych

1. Przetwarzanie Danych osobowych przez Administratora danych odbywa się:
   - przy wykorzystaniu systemów informatycznych oraz
   - poza systemem, w wersji papierowej.

2. Za obszar przetwarzania danych należy rozumieć obszar, w którym wykonywana jest choćby jedna z czynności przetwarzania danych osobowych.

§ 7
Środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzania danych – ogólny opis rozwiązań

1. Zabezpieczenia organizacyjne :

a) sporządzono i wdrożono Politykę Bezpieczeństwa;
b) sporządzono i wdrożono Instrukcję zarządzania systemem informatycznym służącym do przetwarzania Danych osobowych;
c) do przetwarzania danych zostały dopuszczone wyłącznie osoby posiadające upoważnienia nadane przez Administratora danych bądź osobę przez niego upoważnioną;
d) stworzono procedurę postępowania w sytuacji naruszenia ochrony Danych osobowych;
e) osoby zatrudnione przy przetwarzaniu danych zostały zaznajomione z przepisami dotyczącymi ochrony Danych osobowych oraz w zakresie zabezpieczeń systemu informatycznego;
f) osoby zatrudnione przy przetwarzaniu Danych osobowych obowiązane zostały do zachowania tajemnicy;
g) Dane osobowe są powierzane do przetwarzania wyłącznie profesjonalnym, zaufanym podmiotom. Obowiązki podmiotów uczestniczących jako procesor w przetwarzaniu danych są określane w umowach powierzenia;

h) opracowano i wdrożono politykę czystego biurka, czystego ekranu, czystych tablic, czystego pulpitu, czystych drukarek, czystych koszy, przyjmowania interesantów;
i) opracowano i wdrożono politykę dotyczącą kluczy;
j) interesanci (i inne osoby nieupoważnione) nie mają możliwości znalezienia się pod nieobecność pracownika w pomieszczeniu, w którym są przechowywane dane osobowe.

2. Zabezpieczenia techniczne:

a) przetwarzanie Danych osobowych dokonywane jest w warunkach zabezpieczających dane przed dostępem osób nieupoważnionych, a w szczególności:
   - dostęp do pomieszczeń, w których przetwarzane są dane osobowe jest ściśle limitowany
   - Spółka stosuje m.in. zabezpieczenia w postaci: podstawowy czujnik ruchu przy wejściu, system alarmowy, monitoring wizyjny,
   - dane osobowe ujęte w segregatorach, innych podobnych nośnikach danych, opisane są w sposób uniemożliwiający identyfikację (brak nazwisk na grzbietach, brak eksponowania segregatorów i innych akcesoriów zawierających opis w postaci danych osobowych)
   - dokumenty przechowywane są dostosowanych, zabezpieczonych szafach (np. akta osobowe przechowywane są zamykanych, metalowych szafach).

b) dokumenty i nośniki informacji zawierające Dane osobowe, które podlegają zniszczeniu, neutralizuje się za pomocą urządzeń do tego przeznaczonych lub dokonując takiej ich modyfikacji, która nie pozwoli na odtworzenie ich treści, aby po dokonaniu usunięcia danych niemożliwa była identyfikacja osób;

c) proces przetwarzania danych w systemie informatycznym został należycie zabezpieczony (szerzej na ten temat w Instrukcji Zarządzania Systemem Informatycznym).

§ 8
Zasada czystego biurka i czystych tablic

1. Na biurkach poszczególnych pracowników powinny znajdować się wyłącznie te dokumenty, które są niezbędne do bieżącej pracy.

2. Po zakończeniu pracy, wszystkie wykorzystywane dokumenty powinny zostać uprzątnięte i zabezpieczone.
3. Należy unikać przechowywania napojów, innych płynnych substancji w bezpośrednim pobliżu dokumentów oraz stacji roboczych komputerów.
4. Po zakończeniu zgromadzenia, zebrania, prezentacji, należy oczyścić wykorzystywane tablice i inne przyrządy, z informacji stanowiących dane osobowe.

§ 9
Zasada czystego kosza

1. Dokumenty zbędne, nieudane wydruki powinny zostać zutylizowane (przed zniszczeniem należy dokładnie ocenić, czy aby na pewno ustały wszelkie podstawy do dalszego przechowania danego dokumentu).
2. Utylizacja powinna nastąpić przy wykorzystaniu właściwych ku temu urządzeń (niszczarek).
3. Za przykład złej praktyki uznaje się ręczne, niestaranne, nazbyt ogólne niszczenie dokumentów i umieszczanie ich w koszu.

§ 10
Zasada czystego ekranu, czystego pulpitu

1. W czasie podejmowania interesantów, na ekranie komputera nie powinny być wyświetlane żadne informacje mogące choćby pośrednio odnosić się do innych osób.
2. Pulpit komputera w systemie operacyjnym nie powinien stanowić docelowego miejsca przechowywania plików (w szczególności, jeżeli z nazw plików można wywnioskować kogo dotyczą).
3. Ekrany komputerów powinny być skierowane w taki sposób, ażeby osoby postronne odwiedzające biuro, nie mogły uzyskać wglądu w dane dla nich nie przeznaczone.
4. W przypadku czasowego opuszczenia stanowiska pracy, automatycznie aktywowane powinny być zabezpieczone hasłem wygaszacze ekranu (szerzej na ten temat w Instrukcji Zarządzania Systemem Informatycznym).

§ 11
Zasada nadzorowania interesantów

1. Interesanci nie mogą być pozostawiani bez nadzoru, w pomieszczeniach, w których przechowywane są dane osobowe.
2. Rozmowa z interesantami odbywa się we właściwych ku temu warunkach, zapewniających poufność wymienianych treści (dedykowane sale spotkań).
3. Każdy pracownik winien reagować na stwierdzony przypadek nieupoważnionego dostępu do przestrzeni, w której przetwarzane są dane osobowe.

§ 12
Zasady dotyczące kluczy

1. Dostęp do kluczy posiadają wyłącznie osoby upoważnione.
2. Przydział kluczy do poszczególnych pomieszczeń, szaf, szuflad jest ściśle powiązany z zakresem udzielonych upoważnień.
3. Wszystkie stosowane klucze muszą być w sposób jednoznaczny opisane.
4. Klucze pozostają pod nadzorem osób upoważnionych. Osoby upoważnione ponoszą odpowiedzialność za przydzielone im klucze.
5. Zabrania się pozostawiania kluczy w szafach, szufladach itp. podczas czasowego choćby opuszczenia stanowiska pracy.

§ 13
Zasada czasowości – praktyczne aspekty stosowania

Jak wskazano, zgodnie z zasadą czasowości Dane osobowe nie powinny być przetwarzane przez okres dłuższy, niż jest to niezbędne z uwagi na cel dla którego zostały zebrane. Ażeby prawidłowo realizować tę zasadę w praktyce należy:

1. Dokonać indywidualnej oceny, przez jaki okres poszczególne dane osobowe powinny być przetwarzane, czy nadal istnieje podstawa do ich przetwarzania;
2. Ocena ta powinna być wszechstronna (a więc powinna uwzględniać nie tylko wskazany wprost cel przetwarzania, lecz również wszelkie inne uzasadnione powinności i ryzyka;
3. Przed podjęciem decyzji o usunięciu lub zwrocie danych osobowych należy więc np.:

- ustalić czy ustała podstawa do dalszego przetwarzania (np. zakończenie umowy z klientem)

- określić czy dane osobowe powinny być dalej przetwarzane z uwagi na fakt, że roszczenia z danej umowy nie uległy jeszcze przedawnieniu;
- zbadać czy istnieją przepisy prawa, które nakazują nam dalsze przetwarzanie danych (np. przepisy ustawy Ordynacja Podatkowa, ustawy o Systemie Ubezpieczeń Społecznych, przepisy regulujące zasady danego projektu).

§ 14
Obowiązki informacyjne i komunikacja

1. Administrator dba o czytelność i styl przekazywanych informacji i komunikacji z osobami, których dane przetwarza.

2. Administrator ułatwia osobom korzystanie z ich praw poprzez różne działania:
- stworzenie powszechnie dostępnej Polityki prywatności umieszczonej na stronie www;
- zredagowanie broszury informacyjnej, dla osób, których dane są przetwarzane;

3. Administrator dokumentuje obsługę obowiązków informacyjnych, zawiadomień i żądań osób. W tym celu, Administrator:

- udostępnia wzory wniosków
- wprowadza w życie „Rejestr wniosków".

§ 15
Żądania osób uprawnionych

Administrator wprowadza proceduralne gwarancje ochrony praw i wolności osób trzecich. W szczególności, Administrator umożliwiać będzie realizację określonych prawem uprawnień osób, których dane przetwarza. Administrator na wiarygodne żądanie, pochodzące od uprawnionej osoby realizuje następujące prawa :

1) Dostęp do danych – Administrator udzieli informacji, czy i w jakim zakresie przetwarza dane; następnie udzieli dostępu do przedmiotowych danych;

2) Kopie danych – Administrator wyda kopie danych i odnotuje fakt pierwszego wydania; kolejne wydanie kopii może wiązać się z koniecznością pobrania kwoty odpowiadającej bezpośrednim kosztom obsługi żądania;

3) Sprostowanie danych – Administrator sprostuje nieprawidłowe, nieaktualne dane;

4) Uzupełnienie danych – Administrator uzupełni, zaktualizuje dane niepełne

5) Usunięcie danych – Administrator usunie dane, w szczególności jeżeli:

   a) dane nie są niezbędne do celów, w których zostały zebrane,
   b) zgoda na ich przetwarzanie została cofnięta, a nie ma innej podstawy prawnej przetwarzania,
   c) osoba wniosła skuteczny sprzeciw względem przetwarzania tych danych,
   d) dane były przetwarzane niezgodnie z prawem,
   e) konieczność usunięcia wynika z obowiązku prawnego,

6) Ograniczenie przetwarzania – Administrator ograniczy przetwarzanie, w szczególności jeżeli:

   a) osoba kwestionuje prawidłowość danych – na okres pozwalający sprawdzić ich prawidłowość,
   b) przetwarzanie jest niezgodne z prawem, a osoba, której dane dotyczą, sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich wykorzystywania,
   c) nie potrzebuje już danych osobowych, ale są one potrzebne osobie, której dane dotyczą, do ustalenia, dochodzenia lub obrony roszczeń,
   d) osoba wniosła sprzeciw względem przetwarzania z przyczyn związanych z jej szczególną sytuacją – do czasu stwierdzenia, czy po stronie administratora zachodzą prawnie uzasadnione podstawy nadrzędne wobec podstaw sprzeciwu.
   W trakcie ograniczenia przetwarzania Administrator przechowuje dane, natomiast nie przetwarza ich (nie wykorzystuje, nie przekazuje), bez zgody osoby, której dane dotyczą, chyba że w celu ustalenia, dochodzenia lub obrony roszczeń, lub w celu ochrony praw innej osoby fizycznej lub prawnej, lub z uwagi na ważne względy interesu publicznego,

7) Przenoszenie danych – Administrator wyda w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego lub przekazuje innemu podmiotowi, jeśli jest to możliwe, dane dotyczące tej osoby,

8) Sprzeciw – Administrator uwzględni sprzeciw (dotyczy to w szczególności sprzeciwu w szczególnej sytuacji oraz sprzeciwu dot. marketingu bezpośredniego).

Każdy wniosek dotyczący wyżej opisanych uprawnień zostanie rzetelnie rozpoznany przez Administratora i spotka się z odpowiedzią. Nie oznacza to, że każdy wniosek będzie mógł zostać uwzględniony.

§ 16

Instrukcja postępowania w przypadku zagrożeń i incydentów zagrażających bezpieczeństwu danych osobowych

1. Instrukcja definiuje katalog zagrożeń i incydentów zagrażających bezpieczeństwu Danych osobowych oraz opisuje sposób reagowania na nie. Celem instrukcji jest minimalizacja skutków wystąpienia incydentów bezpieczeństwa, ograniczenie ryzyka powstania zagrożeń i występowania incydentów w przyszłości.
2. Każdy pracownik w przypadku stwierdzenia zagrożenia lub naruszenia ochrony Danych osobowych, zobowiązany jest niezwłocznie poinformować Administratora danych.
3. Do typowych zagrożeń bezpieczeństwa Danych osobowych należą:
    1) niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów,
    2) niewłaściwe zabezpieczenie sprzętu, oprogramowania przed wyciekiem, kradzieżą i utratą Danych osobowych,
    3) nieprzestrzeganie zasad ochrony Danych osobowych przez pracowników.
4. Do typowych incydentów bezpieczeństwa Danych osobowych należą:
    1) zdarzenia losowe zewnętrzne (pożar obiektu/pomieszczenia, zalanie wodą, utrata zasilania, utrata łączności),
    2) zdarzenia losowe wewnętrzne (awarie serwera, komputerów, twardych dysków, oprogramowania, pomyłki informatyków, użytkowników, utrata/ zagubienie danych),
    3) 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).
5. W przypadku stwierdzenia wystąpienia zagrożenia, Administrator danych prowadzi postępowanie wyjaśniające w toku, którego:
    1) ustala zakres i przyczyny zagrożenia oraz jego ewentualne skutki,
    2) inicjuje ewentualne działania dyscyplinarne,
    3) rekomenduje działania prewencyjne (zapobiegawcze) zmierzające do eliminacji zagrożeń w przyszłości,
    4) dokumentuje prowadzone postępowania.

6. W przypadku stwierdzenia incydentu (naruszenia) Administrator danych prowadzi postępowanie wyjaśniające w toku, którego:
    1) ustala czas wystąpienia naruszenia, jego zakres, przyczyny, skutki oraz wielkość szkód, które zaistniały,
    2) zabezpiecza ewentualne dowody,
    3) ustala osoby odpowiedzialne za naruszenie,
    4) podejmuje działania naprawcze (usuwa skutki incydentu i ogranicza szkody),
    5) inicjuje działania dyscyplinarne,
    6) wyciąga wnioski i rekomenduje działania korygujące zmierzające do eliminacji podobnych incydentów w przyszłości,
    7) dokumentuje prowadzone postępowania.
7. 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 Prezesowi Urzędu Ochrony Danych Osobowych.
8. Obowiązek, o którym mowa w ust. 7 nie powstaje, jeżeli jest mało prawdopodobne, by odnotowany incydent skutkował ryzykiem naruszenia praw lub wolności osób fizycznych.
9. Zgodnie z literą prawa, zgłoszenie powinno zawierać:
    a) opis charakteru 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) imię i nazwisko oraz dane kontaktowe wyznaczonej u Administratora osoby, która będzie w stanie udzielić bardziej szczegółowych informacji;
    c) opis możliwych konsekwencje naruszenia ochrony Danych osobowych;
    d) opis zastosowanych lub proponowanych przez Administratora środków w celu zaradzenia naruszeniu ochrony Danych osobowych
10. W przypadku przekroczenia terminu 72 h, zgłoszenie musi zawierać precyzyjne określenie przyczyn opóźnienia.
11. Administrator, w oparciu o przewidziane prawem kryteria, dokonuje oceny, czy zachodzi konieczność poinformowania o incydencie, osób których dany problem dotyczy.
12. Wszelkie podmioty, które przetwarzają Dane osobowe na zlecenie Administratora powinny zostać pouczone o obowiązku niezwłocznego informowania o wszelkich incydentach.

§ 17
Zadania Administratora Danych

1. Do najważniejszych obowiązków Administratora Danych należy:
a) organizacja bezpieczeństwa i ochrony Danych osobowych zgodnie z wymogami ustawy o ochronie danych osobowych,
b) zapewnienie przetwarzania danych zgodnie z uregulowaniami Polityki,
c) wydawanie i anulowanie upoważnień do przetwarzania Danych osobowych,
d) prowadzenie ewidencji osób upoważnionych do przetwarzania Danych osobowych,
e) prowadzenie postępowania wyjaśniającego w przypadku naruszenia ochrony Danych osobowych, prowadzenie postępowania wyjaśniającego w przypadku naruszenia ochrony Danych osobowych,
f) nadzór nad bezpieczeństwem Danych osobowych,
g) kontrola działań komórek organizacyjnych pod względem zgodności przetwarzania danych z przepisami o ochronie Danych osobowych,
h) inicjowanie i podejmowanie przedsięwzięć w zakresie doskonalenia ochrony Danych osobowych,
i) Zawiadamianie organu nadzoru w przypadkach przewidzianych prawem.

2. Pamiętać należy, że odpowiedzialność za przetwarzanie Danych osobowych nie obciąża wyłącznie Administratora. Zgodnie z powszechnie obowiązującymi przepisami prawa, sankcje za uchybienia mogą dotknąć wprost osób zatrudnionych (odpowiedzialność dyscyplinarna, możliwość regresu).

§ 18
Postanowienia końcowe

1. Administrator danych ma obowiązek zapoznać z treścią Polityki każdego pracownika.
2. Wszelkie zmiany niniejszego dokumentu będą publikowane w sposób zwyczajowo przyjęty u Administratora danych.