POLITYKA BEZPIECZEŃSTWA INFORMACJI

W ZAKRESIE PRZETWARZANIA DANYCH OSOBOWYCH

W FIRMIE

TK BATO SP. Z O.O.

Spis treści

Rozdział I. Cel Polityki bezpieczeństwa danych osobowych

1. Celem niniejszego dokumentu jest zapewnienie zgodności procesu przetwarzania Danych osobowych w firmie TK BATO Sp. z o.o. z obowiązującymi przepisami prawa, w szczególności z Rozporządzeniem 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 Ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych.
2. Nadrzędnym celem wprowadzonych regulacji wewnętrznych jest zapewnienie przetwarzania Danych osobowych w firmie TK BATO Sp. z o.o. w sposób gwarantujący ich bezpieczeństwo, w szczególności ochronę przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem przepisów prawa, zmianą, utratą, uszkodzeniem lub zniszczeniem.
3. Niniejszy dokument zawiera określenie środków i sposobów ochrony Danych osobowych przyjętych przez firmę TK BATO Sp. z o.o.. Zmiany organizacyjne, zmiany sposobu działania firmy TK BATO Sp. z o.o. w zakresie mającym wpływ na proces przetwarzania Danych osobowych oraz zmiany przepisów prawa będą powodowały konieczność aktualizacji niniejszego dokumentu.

Rozdział II. Zakres stosowania dokumentu

1. Niniejszą Politykę stosuje się w odniesieniu do wszelkich Danych osobowych, wobec których firmie TK BATO SP. z o.o. przysługuje status Administratora Danych, przetwarzanych zarówno w systemach informatycznych jak i w systemach tradycyjnych (papierowych) tj. księgach, skorowidzach, wykazach i innych zbiorach ewidencyjnych, w szczególności Danych osobowych przetwarzanych w celach rekrutacyjnych, zatrudnienia i nawiązania współpracy, finansowych i rachunkowych, marketingowych, handlowych oraz windykacyjnych.
2. Niniejszy dokument podlega przeglądom i aktualizacji, w szczególności w przypadku wystąpienia zmian w przepisach prawa oraz w przypadku wprowadzania zmian w działaniach firmy TK BATO Sp. z o.o. związanych z przetwarzaniem Danych osobowych

- Zakresy określone przez dokumenty Polityki Bezpieczeństwa Informacji mają zastosowanie do całego systemu informacyjnego Firmy, w szczególności do:

1. Wszystkich istniejących, wdrażanych obecnie lub w przeszłości systemów informatycznych oraz papierowych, w których przetwarzane są informacje podlegające ochronie
2. Wszystkich lokalizacji – budynków i pomieszczeń, w których są lub będą przetwarzane informacje podlegające ochronie,
3. Wszystkich pracowników w rozumieniu przepisów Kodeksu Pracy, mających dostęp do informacji podlegających ochronie

- Do stosowania zasad określonych przez dokumenty Polityki Bezpieczeństwa zobowiązani są wszyscy pracownicy w rozumieniu Kodeksu Pracy, mający dostęp do informacji podlegających ochronie.

Rozdział III. Terminologia i skróty

- Zastosowane w niniejszym dokumencie pojęcia i skróty oznaczają:

1. **Administrator Danych** – podmiot decydujący o celach i środkach przetwarzania Danych osobowych – TK BATO Sp. z o.o.
2. **Dane osobowe** – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub klika specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne. Informacji nie uważa się za umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu lub działań.
3. **Hasło** - ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w Systemie informatycznym.
4. **Identyfikator użytkownika** - ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania Danych osobowych w danym Systemie informatycznym.
5. **Obszar przetwarzania danych osobowych** - wykaz budynków, pomieszczeń lub części pomieszczeń, w których odbywa się przetwarzanie Danych osobowych, wobec których status Administratora Danych przysługuje firmie TK BATO Sp. z o.o.
6. **Polityka** – Polityka bezpieczeństwa danych osobowych w firmie TK BATO Sp. z o.o.
7. **Poufność** - właściwość zapewniająca, że Dane osobowe nie są udostępniane nieupoważnionym podmiotom.
8. **Rozliczalność** - właściwość zapewniająca, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi.
9. **Integralność** - właściwość zapewniająca, że Dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany.
10. **System informatyczny** – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania Danych osobowych.
11. **Uwierzytelnianie** - działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu.
12. **Użytkownik** - osoba, która zgodnie z obowiązującymi w firmie TK BATO Sp. z o.o. regulacjami wewnętrznymi otrzymała upoważnienie oraz uprawnienia i Hasła dostępu do pracy w Systemie informatycznym.
13. **Zbiór danych osobowych** – każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie.

Rozdział IV. Zarządzanie ochroną danych osobowych

1. Wszystkie osoby, których rodzaj wykonywanej pracy będzie wiązał się z dostępem do danych osobowych, przed przystąpieniem do pracy, podlegają przeszkoleniu w zakresie obowiązujących przepisów prawa dotyczących ochrony danych osobowych oraz obowiązujących w firmie zasad ochrony danych osobowych.
2. Za bieżącą, operacyjną ochronę danych osobowych odpowiada każda osoba przetwarzająca te dane w zakresie zgodnym z upoważnieniem oraz rolą sprawowaną w procesie przetwarzania danych.
3. Każda z osób mająca styczność z danymi jest zobowiązana do ochrony danych osobowych oraz do przetwarzania ich w granicach udzielonego jej upoważnienia.
4. Należy zapewnić poufność, integralność i rozliczność przetwarzanych danych osobowych.
5. Należy stosować adekwatny do zmieniających się warunków i technologii poziom bezpieczeństwa przetwarzania danych osobowych.
6. Dane osobowe powinny być chronione przed nieuprawnionym dostępem i modyfikacją.

Rozdział V. Obszar przetwarzania danych osobowych

Obszar przetwarzania danych osobowych w firmie TK BATO Sp. z o.o. przedstawia się następująco:

Budynek biurowy TK BATO Sp. z o.o., na który składają się pomieszczenia biurowe firmy.

Rozdział VI. Zbiory danych osobowych i systemy informatyczne wykorzystywane do ich przetwarzania

1. Wykaz Zbiorów danych osobowych oraz Systemów informatycznych służących do ich przetwarzania, wraz z dodatkową informacją o innej formie przetwarzania, w firmie TK BATO Sp. z o.o. przedstawia się następująco:

Lp.	Nazwa Zbioru danych osobowych	Podstawa prawna funkcjonowania zbioru	Forma prowadzenia	Aplikacja	Lokalizacja bazy danych	Miejsce przetwarzania danych
1.	Rekrutacja	Zgodnie z obowiązującymi przepisami	Dokumentacja w formie elektronicznej i papierowej	Poczta elektroniczna	Pomieszczenie biura/stacje robocze	Pomieszczenie biura/stacje robocze
2.	Pracownicy	Zgodnie z obowiązującymi przepisami	Dokumentacja w formie elektronicznej i papierowej	System bankowości elektronicznej, Płatnik ZUS, system Hermes, e-deklaracje	Pomieszczenie biura/pomieszczenie księgowości/stacje robocze	Pomieszczenie biura/pomieszczenie księgowości/stacje robocze
3.	Księgowość	Zgodnie z obowiązującymi przepisami	Dokumentacja w formie elektronicznej	System bankowości elektronicznej, Płatnik ZUS, e-	Pomieszczenie księgowości	Pomieszczenie księgowości/stacje robocze

			i papierowej	deklaracje, poczta elektroniczna, system Hermes		
4.	Kontrahenci	Zgodnie z obowiązującymi przepisami	Dokumentacja w formie elektronicznej i papierowej	Poczta elektroniczna, system bankowości elektronicznej, strona www, sklep internetowy, system Hermes	Pomieszczenie biura/stacje robocze	Pomieszczenie biura/stacje robocze
5.	Korespondencja i dane kontaktowe	Zgodnie z obowiązującymi przepisami	Dokumentacja w formie elektronicznej i papierowej	Poczta Polska, poczta elektroniczna, formularz kontaktowy strony www, system Hermes	Pomieszczenie biura/stacje robocze	Pomieszczenie biura/stacje robocze

Rozdział VII. Środki zapewniające poufność, integralność i rozliczalność przetwarzanych danych osobowych

1. Mechanizmy ochrony organizacyjnej i formalnej:
    1) wprowadzenie dokumentacji przetwarzania Danych osobowych:
        a) Polityka bezpieczeństwa danych osobowych w firmie TK BATO Sp. z o.o.
    2) nadanie upoważnień do przetwarzania Danych osobowych,
    3) prowadzenie szkoleń z zakresu ochrony Danych osobowych dla osób po raz pierwszy upoważnianych do przetwarzania Danych osobowych oraz szkoleń okresowych.

2. Mechanizmy ochrony informatyczno-technicznej:
    1) mechanizmy Uwierzytelnienia Użytkowników z wykorzystaniem unikalnych Identyfikatorów i Haseł,
    2) mechanizmy Rozliczalności operacji realizowanych przez Użytkowników,
    3) połączenie sieci TK BATO Sp. z o.o. z wykorzystaniem zapór sieciowych,
    4) system ochrony antywirusowej,
    5) system ochrony antyspamowej,
    6) systemy monitorujące działania infrastruktury informatycznej pod kątem wykrywania podatności na włamania,
    7) zarządzanie kontami Użytkowników za pomocą domeny,

3. Mechanizmy ochrony fizycznej:
    1) ochrona fizyczna obiektu,
    2) Drzwi wejściowe do obiektu zabezpieczone kodem dostępu z alarmem, zamykane na klucz
    3) system kontroli dostępu z wbudowaną funkcją Rozliczalności,

4) dostęp do pomieszczeń szczególnie chronionych (np. serwerownie) jest ograniczony wyłącznie do osób ściśle upoważnionych,

5) system zasilania awaryjnego wraz z generatorami prądu,

6) serwerownia wyposażona w niezależny UPS,

7) zapewnienie dostępu do niszczarek służących do niszczenia zbędnych, bieżących dokumentów,

8) zapewnienie dostępu do szaf zamykanych na klucz.

Rozdział VIII. Postępowanie w sytuacji naruszenia bezpieczeństwa danych osobowych

1. Każdy użytkownik w przypadku stwierdzenia zagrożenia lub naruszenia ochrony danych osobowych, zobowiązany jest o tym poinformować Administratora Danych,
2. Do typowych zagrożeń bezpieczeństwa danych osobowych należą:
   a) Niewłaściwe zabezpieczenie fizyczne pomieszczeń,
   b) Niewłaściwe zabezpieczenie sprzętu, oprogramowania przed wyciekiem, kradzieżą i utrata danych osobowych,
   c) Nieprzestrzeganie zasad ochrony danych osobowych przez pracowników,
3. Do typowych incydentów bezpieczeństwa danych osobowych należą:
   a) Zdarzenie 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 zagrożenia, Administrator Danych prowadzi postępowanie wyjaśniające w toku którego:
   a) Ustala zakres i przyczyny zagrożenia oraz jego ewentualne skutki,
   b) Inicjuje ewentualne działanie dyscyplinarne,
   c) Rekomenduje działania prewencyjne (zapobiegawcze) zmierzające do eliminacji podobnych zagrożeń w przyszłości,
   d) Dokumentuje prowadzone postępowania,
5. W przypadku stwierdzenia incydentu (naruszenia), Administrator Danych prowadzi postępowanie wyjaśniające, w toku którego:
   a) Ustala czas wystąpienia naruszenia, jego zakres, przyczyny, skutki oraz wielkość szkód, które zaistniały,
   b) Zabezpiecza ewentualne dowody,
   c) Ustala osoby odpowiedzialne za naruszenie,
   d) Podejmuje działania naprawcze (usuwa skutki incydentu i ogranicza szkody)
   e) Inicjuje działania dyscyplinarne,
   f) Wyciąga wnioski i rekomenduje działania korygujące zmierzające do eliminacji podobnych incydentów w przyszłości,
   g) Dokumentuje prowadzone postępowania zgodnie ze wzorem Raportu z naruszenia bezpieczeństwa danych osobowych stanowiący załącznik nr do Polityki Bezpieczeństwa

Rozdział IX Postanowienia końcowe

1. Administrator Danych ma obowiązek zapoznać z treścią Polityki każdego użytkownika,
2. Wszystkie regulacje dotyczące systemów informatycznych, określone w Polityce dotyczą również przetwarzania danych osobowych w bazach prowadzonych w jakiejkolwiek innej formie,
3. Użytkownicy zobowiązani są do stosowania przy przetwarzaniu danych osobowych postanowień zawartych w Polityce,
4. Wobec osoby, która w przypadku naruszenia bezpieczeństwa systemu informatycznego lub uzasadnionego domniemania takiego takiego naruszenia nie podjęła działania określonego w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z okresowymi zasadami, także gdy nie zrealizowała stosownego działania dokumentującego ten przypadek, można wszcząć postępowanie dyscyplinarne,
5. W celu wykonania swoich praw, proszę skierować żądanie pod adres e-mail: odo@bato.pl