POLITYKA BEZPIECZEŃSTWA

w zakresie przetwarzania danych osobowych

Administrator danych osobowych – Baltech Solution sp.z o.o. z siedzibą w Opolu, NIP 7543354094, REGON 523469976 (zwana dalej: Przedsiębiorcą) w celu zapewnienia ochrony przetwarzania danych osobowych, wprowadza poniższą Politykę Bezpieczeństwa. Celem Polityki Bezpieczeństwa danych osobowych, zwanej dalej Polityką Bezpieczeństwa, jest uzyskanie optymalnego i zgodnego z wymogami obowiązujących aktów prawnych, sposobu przetwarzania informacji zawierających dane osobowe.

Przepisy ogólne

1. Obszarem przetwarzania danych osobowych jest wydzielone pomieszczenie w siedzibie Przedsiębiorcy.
2. Dane osobowe powinny być zabezpieczone przed:
   1) udostępnieniem osobom nieuprawnionym;
   2) zabraniem przez osobę nieuprawnioną;
   3) przetwarzaniem z naruszeniem ustawy;
   4) zmianą, utratą, uszkodzeniem lub zniszczeniem danych osobowych.
3. Przedsiębiorca przechowuje dane nie dłużej niż jest to niezbędne dla celu, w jakim są przetwarzane, nie dłużej niż 10 lat.
4. Przetwarzanie danych osobowych do celów związanych z działalnością Przedsiębiorcy jest zgodne z prawem w

sytuacji, gdy dane te zostały uzyskane od osoby, której dotyczą i wyraziła ona na ich przetwarzanie zgodę.

5. W sytuacji, gdy dane osobowe nie zostały uzyskane od osoby, której dotyczą, ich przetwarzanie jest zgodne z prawem, gdy przepis szczególny tak stanowi.
6. Usunięcie danych nie wymaga zgody osoby, której dotyczą.
7. Dokumenty Polityki Bezpieczeństwa ustanawiają metody zarządzania oraz wymagania niezbędne do zapewnienia skutecznej i spójnej ochrony przetwarzania danych.

Uprawnienia osoby, której dane dotyczą

Każdej osobie przysługuje prawo do kontroli przetwarzania danych, które jej dotyczą.

Archiwizowanie informacji zawierających dane osobowe

Archiwizację dokumentów zawierających dane osobowe prowadzi się w odpowiednio zabezpieczonych pomieszczeniach i na właściwie zabezpieczonych nośnikach informatycznych lub tradycyjnych. Dane zbędne dla prowadzonych spraw są natychmiast niszczone poprzez działania fizyczne i informatyczne uniemożliwiające ich odczytanie.

Zmiany w Polityce Bezpieczeństwa

Wszelkie zmiany powyższej instrukcji wprowadzane przez Administratora skuteczne są wobec wszystkich osób, których dotyczą, z chwilą ich doręczenia tym osobom na piśmie.

Postanowienia końcowe

1. Administrator okresowo będzie analizował zagrożenia i ryzyko w celu weryfikacji środków zabezpieczających, a także dokonywał inwentaryzacji systemów informatycznych i zbiorów danych w celu zapewnienia aktualności opisowi zawartemu w Polityce Bezpieczeństwa.

2. Polityka Bezpieczeństwa wchodzi w życie z dniem podpisania.