POLITYKA BEZPIECZEŃSTWA

Administrator Danych

Monika Smaruj

prowadzący działalność gospodarczą pod firmą:

Smaruj Na Trening

Gdańsk

SPIS TREŚCI

1. WSTĘP

1. INFORMACJE OGÓLNE

1. Głównym celem wprowadzenia Polityki Bezpieczeństwa jest zapewnienie zgodności działania Administratora Danych, tj. Monika Smaruj prowadzący działalność gospodarczą pod firmą: Smaruj Na Trening, pod adresem: ul. Słoneczna Dolina 22c/3, 80-126 Gdańsk, NIP: 6070005247, zwanego dalej również „**Administratorem**" z Ustawą o ochronie danych osobowych, Ogólnym Rozporządzeniem o Ochronie Danych (RODO) oraz ich aktami wykonawczymi.

2. ZAKRES INFORMACJI OBJĘTYCH POLITYKĄ BEZPIECZEŃSTWA ORAZ ZAKRES ZASTOSOWANIA

1. Dokument Polityki Bezpieczeństwa opisuje zasady i procedury przetwarzania danych osobowych i ich zabezpieczenia przed nieuprawnionym dostępem.

2. Zakres danych osobowych przetwarzanych przez Administratora, obejmuje dane użyteczne w ramach działalności prowadzonej przez Administratora Danych, w tym przede wszystkim dane osób aplikujących, współpracujących na zasadzie B2B, zleceniobiorców i klientów i inne.

3. Dane są przetwarzane za pomocą systemów teleinformatycznych używanych przez Administratora oraz w biurze Administratora.

2. OSOBY ODPOWIEDZIALNE ZA OCHRONĘ DANYCH OSOBOWYCH

2.1. INFORMACJE OGÓLNE

1. Osobą odpowiedzialną za ochronę danych osobowych jest Administrator, a w razie późniejszego zaangażowania również jego pracownicy oraz osoby współpracujące na podstawie umów o świadczenie usług.

2.2. OSOBY UPOWAŻNIONE DO PRZETWARZANIA DANYCH OSOBOWYCH

1. Każda osoba, która uzyskała upoważnienie do przetwarzania danych osobowych zobowiązana jest do ich ochrony w sposób zgodny z przepisami Ustawy, RODO, Polityki Bezpieczeństwa oraz Instrukcji zarządzania systemem informatycznym.

2. Osoba upoważniona zobowiązana jest do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia. Obowiązek ten istnieje także po ustaniu zatrudnienia.

3. OGÓLNE ZASADY BEZPIECZEŃSTWA OBOWIĄZUJĄCE PRZY PRZETWARZANIU DANYCH OSOBOWYCH

1. Za bezpieczeństwo przetwarzania danych osobowych w określonym zbiorze, indywidualną odpowiedzialność ponosi przede wszystkim każda osoba mająca dostęp do danych osobowych.

2. Dla zapewnienia bezpieczeństwa danych osobowych, Administrator wdrożył działania polegające na przeszkoleniu pracowników i osób ściśle współpracujących ze Administratorem w zakresie zasad bezpieczeństwa i ochrony danych osobowych oraz zapoznała te osoby z niniejszą Polityką Bezpieczeństwa. Administrator powierzać będzie przetwarzanie danych osobowych wyłącznie na podstawie umowy powierzenia zawartej w formie pisemnej.

3. W ramach ochrony danych osobowych zobowiązuje się pracowników i osoby ściśle współpracujące z Administratorem do nieujawniania informacji poufnych i danych osobowych w zakresie w jakim mogłoby to stanowić naruszenie przepisów obowiązującego prawa, a ponadto niniejszym zobowiązuje się wyżej wymienione osoby do:

   - dbałości o brak dostępu osób z zewnątrz do dokumentów znajdujących się w biurze Administratora, a zawierających dane osobowe;
   - zmiany haseł do kont email i logowania do komputerów na których znajdują się dane osobowe;
   - zachowania szczególnej ostrożności podczas przesyłania danych osobowych, w tym dokładnego sprawdzenia poprawności wpisanych adresów email adresatów korespondencji;
   - zamykanie na klucz pomieszczeń, w których znajdują się zbiory danych osobowych, przed opuszczeniem tych pomieszczeń;
   - posiadania i instalowania na elektronicznych nośnikach danych zawierających dane osobowe Administratora wyłącznie legalnego oprogramowania, w tym oprogramowania pełniącego funkcję ochronną przed atakami mającymi na celu kradzież danych.

4. Dostęp do pomieszczeń, w których przetwarzane są zbiory danych osobowych objęte są systemem kontroli dostępu.

5. Administrator będzie, w miarę potrzeb dokonywała czynności wewnętrznych sprawdzających lub kontrolnych w zakresie ochrony danych osobowych. Każda osoba mająca dostęp do danych osobowych nie może ich ujawniać zarówno w miejscu pracy, jak i poza nim, w sposób wykraczający poza czynności związane z ich przetwarzaniem w zakresie obowiązków służbowych lub umownych, w ramach udzielonego upoważnienia do przetwarzania danych.

6. W miejscu przetwarzania danych osobowych utrwalonych w formie papierowej osoby mające dostęp do danych osobowych zobowiązane są do stosowania zasady tzw. „czystego biurka”. Zasada ta oznacza nie

pozostawianie materiałów zawierających dane osobowe w miejscu umożliwiającym fizyczny dostęp do nich osobom nieuprawnionym.

7. Niszczenie brudnopisów, błędnych lub zbędnych kopii materiałów zawierających dane osobowe musi odbywać się w sposób uniemożliwiający odczytanie zawartej w nich treści, np. z wykorzystaniem niszczarek.
8. Niedopuszczalne jest wynoszenie materiałów zawierających dane osobowe poza obszar ich przetwarzania bez związku z wykonywaniem czynności służbowych. Za bezpieczeństwo i zwrot materiałów zawierających dane osobowe odpowiada w tym przypadku osoba dokonująca ich wyniesienia oraz jej bezpośredni przełożony.
9. Przebywanie osób nieuprawnionych w pomieszczeniu, w którym przetwarzane są dane osobowe jest dopuszczalne tylko w obecności osoby upoważnionej do przetwarzania danych osobowych, chyba że dane te są w odpowiedni sposób zabezpieczone przed dostępem.

1. INSTRUKCJA POSTĘPOWANIA W SYTUACJI NARUSZENIA OCHRONY DANYCH OSOBOWYCH

1. Każda osoba, która poweźmie wiadomość w zakresie naruszenia bezpieczeństwa danych przez osobę przetwarzającą dane osobowe bądź posiada informacje mogące mieć wpływ na bezpieczeństwo danych osobowych, ich ujawnienie lub inne naruszenie zasad bezpieczeństwa danych osobowych lub przepisów powszechnie obowiązujących dotyczących ochrony danych osobowych, jest zobowiązana fakt ten niezwłocznie zgłosić do Administratora lub osobie przez Administratora w tym celu wyznaczonej.

2. Do czasu przybycia na miejsce naruszenia ochrony danych osobowych Administratora lub upoważnionej przez Administratora osoby, osoba powiadamiająca powinna:

   - niezwłocznie podjąć czynności niezbędne dla powstrzymania niepożądanych skutków, a następnie ustalić przyczyny, lub sprawców zaistniałego zdarzenia, jeżeli jest to możliwe,
   - zaniechać dalszych planowanych przedsięwzięć, które wiążą się z zaistniałym naruszeniem i mogą utrudnić jego udokumentowanie i analizę,
   - udokumentować wstępnie zaistniałe naruszenie,
   - nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia.

3. Po przybyciu na miejsce naruszenia ochrony danych osobowych Administrator lub upoważniona przez Administratora osoba lub osoba ich zastępująca:

   - zapoznaje się z zaistniałą sytuacją i dokonuje wyboru metod dalszego postępowania
   - wysłuchuje relacji osoby zgłaszającej z zaistniałego naruszenia, jak również relacji każdej innej osoby, która może posiadać informacje związane z zaistniałym naruszeniem,

4. Administrator lub upoważniona przez Administratora osoba dokumentuje zaistniały przypadek naruszenia.

5. Po wyczerpaniu niezbędnych środków doraźnych po zaistniałym naruszeniu, Administrator lub upoważniona przez Administratora osób, zasięga niezbędnych opinii i proponuje postępowanie naprawcze (w tym ustosunkowuje się do kwestii ewentualnego odtworzenia danych z zabezpieczeń) i zarządza termin wznowienia przetwarzania danych, a także, o ile obowiązek taki wynika z powszechnie obowiązujących przepisów prawa, zgłasza naruszenie odpowiedniemu organowi państwowemu ds. ochrony danych osobowych.