Rejestr czynności przetwarzania

I Administrator

1. Administratorem danych jest firma Samaai Spółka z ograniczoną odpowiedzialnością z siedzibą w Bydgoszczy przy ul. Józefa Sułkowskiego 34/4 nr KRS 0000825773 oraz NIP 967 143 31 04 (zwana dalej: „Firmą)

II Cele przetwarzania danych

1. sprzedaż Usług będących przedmiotem oferty
2. doręczanie mailingów informacyjnych i reklamowych
3. organizowanie wyjazdów, warsztatów, eventów sportowych
4. organizacja zajęć sportowych
5. działalność związana ze sportem i zdrowym trybem życia

III Kategoria osób, których dane są przetwarzane

Firma przetwarza dane klientów oraz pracowników, osób samozatrudnionych oraz innych podmiotów współpracujących, w tym również podmiotów zewnętrznych.

IV Kategorie podmiotów, które posiadają dostęp do danych

Do danych osobowych mają dostęp wszyscy członkowie zespołu Firmy. Dostępy do poszczególnych kategorii osób rozdzielone są poprzez ograniczenie uprawnień technicznych wejścia do wspólnego dysku lub ograniczenie dostępu do odpowiednich segregatorów.

Zewnętrznie do danych osobowych dostęp mają następujące podmioty – Google LLC (w tym Google Drive, Gmail) z siedzibą w USA, polityka prywatności: https://policies.google.com/privacy?hl=pl, Facebook Inc. z siedzibą w USA, polityka prywatności: https://www.facebook.com/privacy/explanation, Fakturomania Sp. z o.o. z siedzibą w Polsce, polityka prywatności: https://fakturomania.pl/cookies, UAB “MailerLite” z siedzibą w Litwie, polityka prywatności: https://www.mailerlite.com/legal/privacy-policy, WebToLearn Sp. z o.o., polityka prywatności: https://webtolearn.pl/regulamin-webtolearn.pdf, pracownicy firmy.

Powyższe podmioty jako znajdujące się w obszarze EOG lub na liście Privacy Shield przestrzegają przepisów z zakresu danych osobowych analogicznych do Rozporządzenia tzw. RODO. Z podmiotami zawarte zostały umowy powierzenia, przeważnie w formie aktualizacji ich regulaminów.

V Kategorie danych

1. Administrator przetwarza następujące dane Klienta:
    a. nazwisko i imiona
    b. numer PESEL
    c. adres e-mail
    d. telefon
    e. adres zamieszkania [kod pocztowy]
    f. wiek

    W przypadku, gdy uczestnikiem zajęć tanecznych są dzieci, przetwarzane są dane zarówno ich jak i ich rodziców.
2. Administrator przetwarza adres e-mail oraz imię odbiorcy newslettera.
3. Dla pracowników zespół przetwarzanych danych wynika z przepisów kadrowych.

VI Przechowywanie danych

1. Dane pracowników oraz osób samozatrudnionych są przechowywane przez okres minimum do czasu przedawnienia terminu ewentualnego roszczenia.
2. Dane pracowników tj. listy płac, karty wynagrodzeń albo inne dowody, na podstawie których następuje ustalenie podstawy wymiaru emerytury lub renty firma zobowiązana jest przechowywać przez okres minimum 10 lat od dnia zakończenia przez ubezpieczonego pracy u danego płatnika.
3. Okres przechowywania danych, nie będzie krótszy aniżeli wynika z obowiązujących przepisów prawa (z ustaw szczególnych) tj. m.in.: ustawy o rachunkowości, ordynacji podatkowej, ustawy o emeryturach i rentach z Funduszu Ubezpieczeń Społecznych, czy ustawy o systemie ubezpieczeń społecznych.
4. Dane odbiorców newslettera przechowywane będą do wniosku o ich usunięcie,
5. Dane Klientów przechowywane będą do upływu okresu przedawnienia roszczeń z ich tytułu.

Firma zobowiązuje się do niszczenia powstałych tymczasowo dokumentów zawierających dane osobowe (np. lista uczestników konkretnego eventu lub zajęć) oraz dbałości o obieg danych i ich minimalizację zgodnie z poniższymi procedurami.

VII Techniczne i organizacyjne środki bezpieczeństwa

1. Przez bezpieczeństwo informacji rozumie się zapewnienie:
   a. uniemożliwienia dostępu do danych osobom trzecim;
   b. uniknięcia nieautoryzowanych zmian w danych;
   c. zapewnienia dostępu do danych, w każdym momencie żądanym przez użytkownika
2. Jako dane podlegające szczególnej ochronie (informacje poufne) rozumie się:

a. informacje o realizowanych kontraktach (zarówno planowane, bieżące jak i historyczne),
b. informacje finansowe Firmy,
c. dane osobowe.

VIII Zasada minimalnych uprawnień W ramach nadawania uprawnień przetwarzanych danych należy stosować zasadę „minimalnych uprawnień", to znaczy przydzielać minimalne uprawnienia, które są konieczne do wykonywania pracy na danym stanowisku.

Przykładowo:
pracując na komputerze PC każdy pracownik powinien posiadać tylko takie uprawnienia jakie są wymagane do realizacji swoich obowiązków (a nie na przykład uprawnienia administracyjne).

IX Zasada zabezpieczeń

System IT Firmy powinien być chroniony celem uzyskania skutecznej ochrony danych.
Przykładowo:
w celu ochrony przed wirusami stosuje się równolegle wiele technik: oprogramowanie antywirusowe, systemy typu firewall, odpowiednią konfigurację systemu aktualizacji Windows.

X Dostęp do danych poufnych na stacjach PC

Dostęp do danych poufnych w LAN realizowany jest na przeznaczonych do tego serwerach.

XI Publiczne udostępnianie infrastruktury IT

Infrastruktura udostępniona publicznie musi być szczególnie zabezpieczona.
Przykładowe środki bezpieczeństwa:

a. separacja od sieci LAN
b. wykonanie hardeningu systemu (zwiększenia bezpieczeństwa oferowanego domyślne przez system)

XII Kopie zapasowe

1. Każde istotne dane (w tym dane poufne) powinny być archiwizowane na wypadek awarii w firmowej infrastrukturze IT.

2. Nośniki z kopiami zapasowymi powinny być przechowywane w miejscu uniemożliwiającym dostęp osobom nieupoważnionym.

3. Okresowo kopie zapasowe muszą być testowane pod względem rzeczywistej możliwości odtworzenia danych.

XIII Dostęp do systemów IT po zakończeniu współpracy

W przypadku rozwiązania współpracy pracownika z Firmą niezwłocznie dezaktywowane są wszelakie jego dostępy w systemach IT oraz w terminie 1 roku od dnia rozwiązania

współpracy dezaktywowane są indywidualnie przyporządkowane do pracownika adresy e-mail.

XIV Zabezpieczenie stacji roboczych

1. Stacje robocze powinny być zabezpieczone przed nieautoryzowanych dostępem osób trzecich. Minimalne środki ochrony to:
    a. zainstalowane na stacjach systemy typu: firewall oraz antywirus,
    b. wdrożony system aktualizacji systemu operacyjnego oraz jego składników,
    c. wymaganie podania hasła przed uzyskaniem dostępu do stacji,
    d. bieżąca praca z wykorzystaniem konta nieposiadającego uprawnień administracyjnych.

XV Wykorzystanie haseł

1. Hasła powinny być okresowo zmieniane.
2. Hasła nie mogą być przechowywane w formie otwartej (nie zaszyfrowanej).
3. Nie wolno przekazywać hasła osobom trzecim.
4. Hasła nie powinny być łatwe do odgadnięcia, to znaczy:
    a. powinny składać się z minimum 8 znaków, w tym jeden znak specjalny, cyfra i wielka litera,
    b. nie może być słowem żadnego języka.

XVI Odpowiedzialność pracowników za dane poufne

Pracownicy zobowiązani są do strzeżenie danych poufnych, w tym osobowych.

XVII Odpowiedzialność pracowników za dane dostępowe do systemów

1. Każdy pracownik zobowiązany jest do ochrony swoich danych dostępowych do systemów informatycznych. Dane dostępowe obejmują między innymi takie elementy jak:
    a. hasła dostępowe,
    b. klucze softwareowe (pliki umożliwiające dostęp - np. *certyfikaty do VPN*) oraz sprzętowe,
    c. inne mechanizmy umożliwiające dostęp do systemów IT.

XVII Przykłady ochrony danych dostępowych

- nieprzekazywanie dostępów do systemów IT innym osobom (np. przekazywanie swojego hasła dostępowego osobom trzecim),
- nieprzechowywanie danych w miejscach publicznych (np. zapisywanie haseł dostępowych w łatwo dostępnych miejscach),
- ochrona danych dostępowych przed kradzieżą przez osoby trzecie.

XVIII Systemy IT/serwery

Systemy IT przechowujące dane poufne (np. dane osobowe) muszą być odpowiednio zabezpieczone. W szczególności należy dbać o poufność, integralność i rozliczalność danych przetwarzanych w systemach.

XIX Dokumentacja papierowa

1. Dokumentacja papierowa zawierająca dane osobowe zamykana jest na klucz. Dostęp do kluczy mają tylko osoby uprawnione, które podpisały oświadczenia o zabezpieczaniu danych osobowych.
2. Osoba odpowiedzialna za księgowość przechowuje wszelką dokumentację papierową zawierającą dane osobowe klientów oraz pracowników Firmy w szafie

zamykanej na klucz. Dostęp do kluczy mają tylko osoby uprawnione, które podpisały oświadczenia o zabezpieczaniu danych osobowych.

3. W przypadku wizyty klienta w siedzibie Firmy nie ma on dostępu do szafek, biurek i drukarek. Preferowane jest „odprowadzanie” do niezawierającej dokumentów sali.

XX Ograniczony dostęp do biura

Dostęp do budynku Firmy jest ograniczony poprzez zamykane na klucz drzwi wejściowe.

XXI Naruszenie danych osobowych

Pracownik zobowiązany jest do poinformowania o naruszeniu w ciągu 24 godzin. O ile wystąpi taka konieczność zgłoszenie naruszenia danych osobowych następuje w ciągu 48

godzin od daty powzięcia informacji o powyżej wymienionym zdarzeniu, zgodnie z poniżej przedstawionym schematem.

XXII Formularze

Raport z naruszenia ochrony danych osobowych w Firmie powinien zawierać następujące informacje:

1. data, godzina
2. dane osoby powiadamiającej o zaistniałym zdarzeniu (imię, nazwisko, stanowisko służbowe, nazwa użytkownika (jeżeli występuje)
3. lokalizacja zdarzenia: (np. numer pokoju, nazwa pomieszczenia, nazwa bazy danych)
4. rodzaj naruszenia bezpieczeństwa
5. podjęte działania
6. przyczyny wystąpienia zdarzenia
7. postępowanie wyjaśniające
8. podjęte środki techniczne, organizacyjne i dyscyplinarne w celu zapobiegania w przyszłości podobnych naruszeń ochrony danych osobowych.

XXIII. Prawo do usunięcia/zmiany danych

Jeśli klient chce usunąć swoje dane przetwarzane przez Firmę powinien stawić się w siedzibie firmy osobiście w celu weryfikacji danych.

Firma usuwa dane z:

1. **fizycznej umowy** *wkładamy do niszczarki i niszczymy*
2. **korespondencji mailowej** *usuwamy tylko taką, w której zawierają się dane osobowe, resztę zachowujemy jako dowód zawarcia transakcji*
3. **systemów IT** *usuwamy tylko takie, w których zawierają się dane osobowe, resztę zachowujemy jako dowód zawarcia transakcji.*
4. **programu fakturowego - *zostawiamy z powodu przepisów ustawy o rachunkowości.***

XXIV Wgląd do danych osobistych

Jeśli jakikolwiek podmiot, którego dane są przetwarzane przez Firmę chce otrzymać wgląd do swoich danych i je poprawić/zaktualizować, powinien stawić się w siedzibie firmy

osobiście w celu weryfikacji danych. Następnie po jego weryfikacji, dane klienta zostaną niezwłocznie zmienione/podane.

XXV Procedura przeniesienia danych klienta

W sytuacji gdy klient zgłosi się z prośbą o przeniesienie jego danych do innej firmy, z którą aktualnie nawiązał współpracę, musi się on zgłosić się osobiście z podaniem adresu e-mail na który mają te dane zostać przez Firmę wysłane, a następnie po jego weryfikacji, dane klienta zostaną niezwłocznie zmienione/podane.