Załącznik – Standardowe środki techniczne i organizacyjne stosowane przez Futuriti

Niniejszy załącznik stanowi opis standardowych środków technicznych i organizacyjnych stosowanych przy świadczeniu usług dla klientów związanych z przetwarzaniem danych osobowych. Umowa główna może (ale nie musi) określać dodatkowe lub inne środki uzgodnione przez strony i w tym zakresie postanowienia Umowy Głównej będą miały postanowienia pierwszeństwo przed postanowieniami niniejszego załącznika.

FUTURITI ma prawo w każdym czasie, bez uprzedzenia, dokonywać modyfikacji stosowanych Standardowych środków technicznych i organizacyjnych w oparciu o zmiany w przepisach, powstanie lub zmianę dobrych praktyk, zmianę możliwości technicznych a także adekwatnie do przedsięwzięcia informacji o występujących zagrożeniach – stosując zasadę należytej staranności i adekwatności zabezpieczeń.

1. Środki techniczne i organizacyjne – kontrola dostępu
    a. Dostęp do miejsc przechowywania i przetwarzania danych posiadają wyłącznie upoważnieni pracownicy i współpracownicy oraz jedynie w sytuacji wyższej konieczności niezbędne służby ratownicze i ochrona.
    b. Dostęp do pomieszczeń FUTURITI jest ograniczony przez indywidualne karty dostępowe lub inne fizyczne metody kontroli dostępu do nieruchomości.
    c. Dostęp do systemów wewnętrznych i środowisk oraz danych klientów możliwy jest tylko dla wybranych upoważnionych pracowników i współpracowników po zalogowaniu na indywidualne konto przy użyciu hasła zgodnego z Polityką haseł. Dostęp do systemu klienta może odbywać się na udostępnione przez klienta konto zbiorcze, dostęp do danych konta zbiorczego jest przechowywany w dedykowanym narzędziu rejestrującym każdorazowe uzyskanie takich danych przez indywidualną osobę.
    d. Zdalny dostęp pracowników lub współpracowników do sieci FUTURITI i późniejsza wymiana odbywa się po uwierzytelnieniu przy zachowaniu kryptograficznych mechanizmów zapewniających poufność i integralność (np. VPN, SSL itp.)
    e. W celu zapewnienia bezpieczeństwa oraz tam gdzie to jest uzasadnione FUTURITI stosuje monitoring oraz współpracuje z zewnętrzną ochroną.
    f. Wszyscy pracownicy oraz współpracownicy dopuszczeni do przetwarzania danych osobowych są pouczeniu o obowiązku zachowania w tajemnicy przetwarzania danych osobowych
    g. Wszyscy pracownicy oraz współpracownicy dopuszczeni do przetwarzania danych osobowych są zapoznani z obowiązującymi przepisami o ochronie danych osobowych
2. Środki techniczne i organizacyjne – bezpieczeństwo i ciągłość dostępu do danych przetwarzanych w FUTURITI jako głównym miejscu przetwarzania danych
    a. Dane przetwarzane w FUTURITI jako głównym miejscu przetwarzania danych to dane przechowywane np. na serwerze VPS udostępnianym przez FUTURITI, w aplikacji hostowanej w FUTURITI jak np. 4Hero, xSale. Danymi takimi nie są dane powierzone w celu wykonania np. usługi serwisowej, weryfikacji błędu itd., dla których można rozsądnie przypuszczać, że są w innym miejscu przetwarzane jako głównym miejscu przetwarzania danych.
    b. Dane ww. podlegają kopii zapasowej (backup) zgodnie z procedurą stosowaną w FUTURITI, backup danych to minimum:
        i. dobowa kopia baz danych na danym serwerze

ii. Replikacja danych całego serwera w trybie ciągłym na osobny serwer fizyczny

c. Serwery i usługi wykorzystywane przez FUTURITI mają zagwarantowane utrzymanie ciągłej dostępności przez:
   i. Stosowanie macierzy RAID w serwerach zapewniającą odporność na awarię pojedynczego dysku twardego
   ii. Stosowanie ciągłej replikacji danych na inne serwery fizyczne w celu krótkiego przywrócenia dostępności po wystąpieniu awarii całego serwera
   iii. FUTURITI stosuje co najmniej dwa równoczesne łącza internetowe umożliwiające pracę po wystąpieniu awarii jednego z nich przy wykorzystaniu protokołu BGP.

d. Dane ww. mogą być przetwarzane wyłącznie na urządzeniach i usługach FUTURITI (w tym nabytych od podmiotów zewnętrznych).

e. W przypadku wykorzystania usług (np. hostingu) od podmiotów zewnętrznych – podmiot ten musi gwarantować co najmniej analogiczny poziom ochrony danych.

f. Dane są przetwarzane wyłącznie na ww. urządzeniu, do którego dostęp fizyczny jest ograniczony przed osobami nieupoważnionymi.

g. Dane są przetworzone wyłącznie na usługach i urządzeniach do których dostęp wymaga indywidualnego zalogowania się.

h. FUTURITI stosuje system IDS (Intrusion Detection System) monitorujący przepływ danych oraz wykrywający określone sygnatury naruszenia bezpieczeństwa wraz z procedurą monitorowania i reagowania na ww.

i. FUTURITI stosuje system Firewall ograniczający dostęp do sieci FUTURITI oraz indywidualny Firewall dla każdego z serwerów.

3. Środki techniczne i organizacyjne – bezpieczeństwo przetwarzania danych, które nie są przetwarzane w FUTURITI jako głównym miejscu przetwarzania danych,
   a. Dane przetwarzane w FUTURITI , których głównym miejscem przetwarzania danych nie jest FUTURITI to np. dane udostępnione do migracji, odtworzenia błędu, udzielenia konsultacji itp., dla których można rozsądnie przypuszczać, że są w innym miejscu przetwarzane jako głównym miejscu przetwarzania danych. Dane takie nie są objęte polityką backupu w FUTURITI .
   b. Dane ww. mogą być przetwarzane wyłącznie na urządzeniach i usługach FUTURITI (w tym nabytych od podmiotów zewnętrznych)
   c. W przypadku wykorzystania usług (np. hostingu) od podmiotów zewnętrznych – podmiot ten musi gwarantować co najmniej analogiczny poziom ochrony danych.
   d. Dane są przetwarzane wyłącznie na ww. urządzeniu, do którego dostęp fizyczny jest ograniczony przed osobami nieupoważnionymi.
   e. Dane są przetworzone wyłącznie na usługach i urządzeniach do których dostęp wymaga indywidualnego zalogowania się.
4. Zarządzanie incydentami bezpieczeństwa
   a. W FUTURITI wdrożona jest procedura zarządzania incydentami naruszenia bezpieczeństwo i nałożono na wszystkich pracowników i współpracowników obowiązek zgłaszania wszelkiego rodzaju incydentów naruszenia bezpieczeństwa jak również incydentów dotyczących naruszenia ochrony danych osobowych.
5. Szkolenia i audyty

a. W FUTURITI wdrożona jest procedura zapewniająca okresowe szkolenie z zakresu obowiązujących procedur bezpieczeństwa i ochrony danych osobowych
b. Audyt bezpieczeństwa systemów wewnętrznych i zewnętrznych wykorzystywanych przez FUTURITI jest przeprowadzany okresowo przez osoby lub podmioty upoważnione i zobowiązane przez Zarząd FUTURITI