Certyfikacja zgodności z RODO - środki techniczne i organizacyjne

Dokument przedstawia ogólny opis środków technicznych i organizacyjnych stosowanych przez firmę BrainSHARE IT sp. z o.o. z siedzibą w Krakowie przy świadczeniu dla klientów usług związanych z przetwarzaniem danych osobowych w związku z korzystaniem z Systemu SaldeoSMART zgodnych z wymaganiami Rozporządzenia 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 uchylenia dyrektywy 95/46/WE (zwane RODO).

W BrainSHARE IT sp. z o.o. (BrainSHARE, Spółka) wdrożone zostały niezbędne procedury i polityki służące m.in. zapewnieniu bezpieczeństwa, poufności, integralności i dostępności danych klientów (w tym danych osobowych, w stosunku do których BrainSHARE jest administratorem czy procesorem), do których w ramach świadczonych usług uzyskują dostęp pracownicy lub współpracownicy Spółki.

1. **Procedury i polityki służące do zapewnienia bezpieczeństwa, poufności i integralności danych osobowych w tym:**
    a. Polityka bezpieczeństwa (sieć, dostęp do pomieszczeń)
    b. Polityka ciągłości działania (Distater Recovery, Polityka Backup)
    c. Standardy dla serwerów i stacji roboczych
2. **Kontrola dostępu**
    a. Ograniczony dostęp do budynków, środowisk, i zbiorów danych wyłącznie dla osób upoważnionych.
    b. Pracownicy lub współpracownicy korzystają z kart dostępowych lub stosowane są inne metody kontroli fizycznego dostępu do nieruchomości, budynków lub pomieszczeń firmy, zapewniające kontrolę dostępu poszczególnych osób odpowiednią do zakresu ich uprawnień.
    c. Nadawanie uprawnień poszczególnym pracownikom lub współpracownikom w zakresie dostępu do systemów wewnętrznych BrainSHARE oraz środowisk klienta podlega procedurze umożliwiającej weryfikację wniosku o nadanie uprawnień.
    d. Dostęp do systemów wewnętrznych i środowisk oraz danych klientów możliwy jest tylko dla upoważnionych pracowników lub współpracowników po zalogowaniu na indywidualne konto i przy użyciu indywidualnego hasła zgodnego z Polityką bezpieczeństwa.
    e. Zdalny dostęp pracowników lub współpracowników do sieci Spółki i późniejsza wymiana informacji odbywają się po uwierzytelnieniu przy wykorzystaniu bezpiecznych mechanizmów, zapewniających poufność i integralność (VPN).
    f. W celu zapewnienia bezpieczeństwa, tam gdzie jest to uzasadnione Spółka współpracuje z firmami ochroniarskimi.
    g. Lista aktualnych podwykonawców - Polcom S.A., współpracownicy B2B.
3. **Środki ochrony programów i baz danych**
    a. Dostęp do zbioru danych osobowych wymaga uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła
    b. Zastosowano kryptograficzne środki ochrony danych osobowych - certyfikat ssl
    c. Zainstalowano wygaszacze ekranów na stanowiskach, na których przetwarzane są dane osobowe.

d. Zastosowano mechanizm automatycznej blokady dostępu do systemu informatycznego służącego do przetwarzania danych osobowych w przypadku dłuższej nieaktywności pracy użytkownika
e. Zastosowano środki ochrony przed szkodliwym oprogramowaniem takim, jak np. robaki, wirusy, konie trojańskie, rootkity.
f. Użyto systemu firewall do ochrony dostępu do sieci komputerowej.

4. **Data Center**

   Serwery, których właścicielem jest Spółka; zlokalizowane są w Polsce poprzez kolokację w firmie Polcom w Alwernii oraz Skawinie pod Krakowem - Certyfikat Bezpieczeństwa Data Center ISO 27001 oraz zgodność z TIER 4.

   a. Kontrola dostępu, monitoring, ochrona fizyczna
   b. Rendundacja klimatyzacji, zasilania energetycznego, łącza telekomunikacyjnego;
   c. Zasilanie zapasowe dla serwerów;
   d. System przeciwpożarowy;
   e. Rendundancja warstwy fizycznej (serwery, urządzenia sieciowe, połączenia FC, Ethernet);
   f. Stosowane są następujące procesy:
      i. Zarządzanie aktualizacjami i łatkami;
      ii. Procedury backupowe i odtworzeniowe zgodnie z Polityką Backupów;
      iii. Wysoka dostępność (HA) na wypadek awarii
   g. Backup środowisk produkcyjnych znajduje się w dwóch różnych lokalizacjach, w tym jeden z nich w osobnej lokalizacji geograficznej, aniżeli system produkcyjny
   h. Wstęp do Data Center mają tylko uprawnione osoby przez Spółkę - uprawnienia dostępu przyznawane są tylko na wniosek Prezesa Zarządu.
   i. Wszelkie fizyczne działania w Data Center są logowane i protokołowane.

5. **System SaldeoSMART**
   a. Daje możliwość nadania każdemu użytkownikowi osobnego loginu;
   b. Wymusza logowanie przy użyciu loginu oraz hasła.
   c. Hasła użytkowników są zapisane w postaci jednokierunkowego skrótu (funkcja haszująca).
   d. Zapewnia dostęp i kontrolę wybranych obszarów danych - poprzez prawa na użytkownikach;

6. **SaldeoSMART - wersja online**
   a. Połączenie z serwerem SaldeoSMART jest szyfrowane (SSL);
   b. Zasoby serwerów chronione są przez Firewall;
   c. Dostęp do maszyn produkcyjnych mają tylko uprawnieni do tego pracownicy lub współpracownicy;
   d. Dane użytkowników oraz bazy danych aplikacji są przechowywane na zaszyfrowanych dyskach;
   e. Przetwarzane dane nie są przekazywane poza Europejski Obszar Gospodarczy.
   f. Zastosowanie mają wszystkie elementy wymienione w pkt. 4.

7. **SaldeoSMART - wersja lokalna**
   a. Połączenie z serwerem SaldeoSMART jest szyfrowane (SSL) w przypadku udostępnienia systemu w sieci publicznej;
   b. Rekomenduje się aby dyski maszyny wirtualnej SaldeoSMART były szyfrowane;

c. Zasoby serwera chronione są przez Firewall;
d. Dostęp do OS maszyny mają tylko uprawnione do tego osoby, a ich działania są logowane;
e. Zapewnienie ciągłości działania i wykonywanie kopii bezpieczeństwa leży w kwestii Administratora Danych (Klienta).
f. BrainSHARE nie przekazuje przetwarzanych danych poza Europejski Obszar Gospodarczy.

8. **Zarządzanie incydentami**

W BrainSHARE wdrożono procedurę zarządzania incydentami naruszenia bezpieczeństwa i nałożono na wszystkich pracowników i współpracowników obowiązek zgłaszania wszelkiego rodzaju incydentów naruszenia bezpieczeństwa, w tym incydentów dotyczących naruszenia ochrony danych osobowy