Klauzula Informacyjna dotycząca danych generowanych przez Produkt Skomunikowany

(zgodnie z art. 3 ust. 2 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2023/2854 z dnia 13 grudnia 2023 r. w sprawie zharmonizowanych przepisów dotyczących sprawiedliwego dostępu do danych i ich wykorzystywania oraz w sprawie zmiany rozporządzenia (UE) 2017/2394 i dyrektywy (UE) 2020/1828 (akt w sprawie danych) (Dz.U. UE. L. z 2023 r. poz. 2854))

Szanowny Użytkowniku,
Niniejsza klauzula informacyjna jest dostarczana przez TermoPlaza Sp. z o.o., ul. Żegańska 21/23, 04-713 Warszawa, KRS: 0000752275 w celu spełnienia wymogów Aktu o Danych i ma na celu zapewnienie przejrzystości w zakresie danych generowanych przez produkt skomunikowany, który zamierzasz nabyć. Prosimy o zapoznanie się z poniższymi informacjami przed zawarciem umowy.
Definicję produktu skomunikowanego spełniają wyłącznie grzejniki TermoPlaza serii WIFI o oznaczeniu modelu "____ WIFI".

1. Rodzaj, format i szacunkowa ilość danych produktu, które produkt skomunikowany jest w stanie wygenerować.

- Rodzaje danych: Produkt skomunikowany jest w stanie generować dane dotyczące jego działania, wykorzystywania i otoczenia. Mogą to być m.in.:
    - Informacje o urządzeniu: nazwa urządzenia, ID urządzenia, status online, czas aktywacji, wersja oprogramowania układowego (firmware).
    - Informacje o konfiguracji sieci: szczegóły Wi-Fi i uprawnienia lokalizacyjne, wykorzystywane wyłącznie do konfiguracji sieci urządzenia i nie są przesyłane do chmury.
    - Logi użytkowania urządzenia: dane z czujników (np. jasność i temperatura barwowa dla inteligentnej lampy, temperatura i wilgotność dla osuszacza) oraz polecenia konfiguracyjne wysyłane z aplikacji do urządzenia.
- Format danych: Dane są zazwyczaj ustrukturyzowane w formacie klucz-wartość. Użytkownicy mają możliwość eksportowania danych w ustrukturyzowanym formacie za pośrednictwem aplikacji.
- Szacunkowa ilość danych: zaledwie kilkadziesiąt KB dziennie.

2. Czy produkt skomunikowany jest w stanie generować dane w sposób ciągły i w czasie rzeczywistym?

Tak, produkty skomunikowane, gdy są online, są w stanie generować dane w sposób ciągły i w czasie rzeczywistym. Częstotliwość zbierania danych jest zazwyczaj w czasie rzeczywistym lub wywoływana zdarzeniami (np. włączenie/wyłączenie inteligentnej wtyczki).

3. Czy produkt skomunikowany jest w stanie przechowywać dane na urządzeniu lub na zdalnym serwerze, w tym w stosownym przypadku zamierzony okres zatrzymywania danych?

Produkty skomunikowane przechowują dane na serwerach chmurowych.
Domyślny okres przechowywania danych z punktów funkcji urządzenia (DataPoint) wynosi 7 dni. Okres ten może zostać przedłużony na żądanie klienta poprzez zakup dodatkowych usług przechowywania. Logi użytkowania urządzenia są przechowywane przez 7 dni, a następnie są automatycznie usuwane.

4. W jaki sposób użytkownik może uzyskać dostęp do tych danych, pobrać je lub w stosownym przypadku usunąć, w tym środki techniczne stosowane w tym celu, a także warunki ich wykorzystywania i jakość usługi?

- Dostęp i eksport danych: Użytkownik może przeglądać i eksportować swoje dane urządzenia za pośrednictwem intuicyjnego interfejsu w aplikacji mobilnej. Proces ten obejmuje następujące kroki:
    - W aplikacji przejdź do sekcji: Ja (Me).
    - Następnie wybierz Ustawienia (Settings) w prawym górnym rogu.
    - Wybierz Zarządzanie polityką prywatności (Privacy Policy Management).
    - Wybierz Eksport danych urządzenia (Device Data Export).
    - Wybierz odpowiednie urządzenie.
    - Wyświetl podgląd danych (Data preview) i dotknij "Eksportuj" (Export) w prawym górnym rogu.
    - Podaj adres e-mail, na który mają zostać wysłane dane.

Aby uzyskać dostęp do tych funkcji, aplikacja powinna być w wersji 6.5.0 lub wyższej. System wspiera przenoszenie danych, umożliwiając ich eksportowanie w ustrukturyzowanym formacie za pośrednictwem aplikacji.

- Usuwanie danych: Użytkownik ma możliwość usunięcia swoich danych w dowolnym momencie poprzez odłączenie urządzenia i wybranie opcji "Usuń dane".
- Środki techniczne i bezpieczeństwa: Dostawca aplikacji (przetwarzający dane) stosuje rygorystyczne środki techniczne i organizacyjne w całym cyklu życia danych (zbieranie, przesyłanie, przechowywanie, dostęp, eksport, usuwanie) w celu zapobiegania nieuprawnionemu dostępowi, modyfikacji lub ujawnieniu. Obejmują one:
    - Szyfrowanie: Szyfrowanie TLS 1.2/1.3 dla danych w transporcie; szyfrowanie AES-256 dla danych w spoczynku.
    - Kontrola dostępu: Kontrola dostępu oparta na rolach (RBAC) i zasadzie najmniejszych uprawnień, z obsługą uwierzytelniania dwuskładnikowego.
    - Ochrona integralności: Wykorzystanie podpisów lub kontroli w celu wykrywania i zapobiegania manipulacji danymi.
    - Audyty bezpieczeństwa i monitorowanie: Monitorowanie dostępu do danych i logów operacji w czasie rzeczywistym, regularne audyty bezpieczeństwa i skanowanie luk.
    - Bezpieczeństwo eksportu i udostępniania: Weryfikacja uprawnień dostępu przed eksportem, a eksportowane dane są przesyłane przez zaszyfrowane kanały.
    - Certyfikaty zgodności: Dostawca aplikacji (przetwarzający dane) utrzymuje międzynarodowe certyfikaty, takie jak ISO 27001, ISO 27701, SOC 2 Type II.
- Warunki wykorzystywania danych: Użytkownik ma prawo wykorzystywać pozyskane dane w każdym zgodnym z prawem celu. Zabrania się jednak wykorzystywania danych do opracowywania produktu skomunikowanego konkurującego z produktem, z którego pochodzą dane, a także udostępniania danych w tym celu osobom trzecim. Nie wolno również wykorzystywać danych do pozyskiwania informacji o sytuacji ekonomicznej, aktywach i metodach produkcji producenta lub posiadacza danych.
- Jakość usługi dostępu do danych: Dostęp do danych jest zapewniony bez zbędnej zwłoki, w sposób łatwy i bezpieczny, a udostępniane dane charakteryzują się taką samą jakością, jaka jest dostępna dla posiadacza danych.