The Enervent group

POLITYKA PRYWATNOŚCI

Sekcje 10 oraz 24 ustawy o ochronie danych osobowych (523/1999)

Nazwa rejestru
eAir WEB

Cel przetwarzania danych osobowych
Portal online systemu sterowania urządzeń wentylacyjnych eAIR

Podmiot zbierający dane
Enervent Oy, Kipinätie 1, FI-06150 Porvoo, Finlandia

Osoba kontaktowa oraz inspektor ochrony danych w Enervent group
Enervent Oy, Kipinätie 1, FI-06150 Porvoo, Sonja Häggman, tel. +358 20 7528 800, e-mail enervent@enervent.com

Organ nadzoru
Biuro inspektora ochrony danych w Finlandii

Profilowanie
Dla danych osobowych nie będzie wykonywane profilowanie oraz automatyczne decyzje indywidualne.

Transfer danych poza obszar UE lub EOG
Dane nie będą transferowane poza obszar EOG.

Prawo do sprawdzenia i poprawienia danych oraz do transferu ich do innego systemu
Każda osoba ma prawo do sprawdzenia i poprawienia swoich danych, które zostały zapisane w rejestrze tej osoby (w odniesieniu do części danych elektronicznych przekazanych przez podmiot danych) oraz do transferu ich do innego systemu. Wnioski: Enervent Oy, Kipinätie 1, FI-06150 Porvoo, Sonja Häggman, tel. +358 20 7528 800, e-mail enervent@enervent.com

Prawo do usunięcia danych
Każda osoba ma prawo do usunięcia swoich danych osobowych z systemu. Wnioski: Enervent Oy, Kipinätie 1, FI-06150 Porvoo, Finlandia
Sonja Häggman, tel. +358 20 7528 800, e-mail enervent@enervent.com

Warunek konieczny do przetwarzania danych osobowych (zgoda, uzasadnione zainteresowanie, umowa lub obowiązek prawny)
Zgoda

Specjalne (wrażliwe) dane osobowe rejestru
Brak

Zwykłe dane osobowe rejestru
Adres IP urządzenia wentylacyjnego oraz ustawienia techniczne, status, dane pomiarowe z urządzenia wentylacyjnego oraz podłączonych czujników.

Źródła danych regularnych
Dane są przesyłane z urządzenia wentylacyjnego.

Regularne udostępnianie danych
Dane te są przechowywane w formie szyfrowanej w usłudze opartej na chmurze dostawcy usługi oraz są dostępne tylko dla podmiotu danych, chyba że upoważnił on firmę Enervent Oy do monitorowania danego urządzenia wentylacyjnego.
Dane te nie będą udostępniane poza Enervent group lub jej spółkę dominującą.

Marketing bezpośredni
Dane osobowe nie mogą być udostępniane poza Enervent group. Jednakże Enervent może użyć tych danych do celów marketingu bezpośredniego po uzyskaniu osobnej zgody.

Okres przechowywania danych
Dane te nie są przeznaczone do usuwania z systemu, ponieważ zawierają one informacje, które sa niezbędne do konserwacji dostarczonych urządzeń wentylacyjnych. Okres żywotności tych urządzeń wentylacyjnych jest liczony w dekadach.

Procesy dotyczące sprawdzania, poprawiania, transferu i usuwania danych osobowych
Gdy podmiot danych zwróci się z wnioskiem o sprawdzenie, poprawienie, transfer lub usunięcie danych osobowych, osoba kontaktowa dla tego rejestru powinna rozpocząć odpowiedni z góry określony proces. Proces ten obejmuje:
1) Poinformowanie podmiotu danych o otrzymaniu wniosku (w ciągu 7 dni od otrzymania wniosku)
2) Określenie działań, które mają zostać podjęte i wybranie osób odpowiedzialnych (w ciągu 14 dni od otrzymania wniosku)
3) Podjęcie określonych działań
4) Udokumentowanie tych działań
5) Poinformowanie podmiotu danych o działaniach, jakie zostały podjęte (w ciągu 30 dni od otrzymania wniosku)

Naruszenia bezpieczeństwa danych

Jeżeli transferowane, zapisane lub w inny sposób przetwarzane dane zostały przypadkowo lub nielegalnie zniszczone, utracone lub zmienione lub zostało wykryte nielegalne udostępnienie lub dostęp do danych, administrator rejestru musi natychmiast powiadomić Prezesa Zarządu o tej sprawie. Prezes Zarządu powinien rozpocząć proces, podczas którego

1) Powinny zostać natychmiast podjęte środki naprawcze w celu uniknięcia dalszych szkód
2) O incydencie tym powinien zostać poinformowany organ nadzoru w ciągu 72 godzin od momentu wykrycia tego naruszenia zgodnie z instrukcjami tego organu.
3) Podmioty danych, których dotyczy to naruszenie, powinny zostać poinformowane o tej sprawie najszybciej jak to możliwe, jeżeli naruszenie to stanowi dla nich zagrożenie
4) Powinny zostać podjęte środki poprawiające mające na celu uniknięcie przyszłych naruszeń bezpieczeństwa danych
5) Organ nadzorczy powinien zostać poinformowany o podjętych działaniach

Zasady ochrony rejestru

Dane w formacie elektronicznym są chronione hasłem i tylko wybrane osoby mają do nich dostęp. Dane w formacie papierowym są przechowywane w zamkniętej szafie, do której klucz mają tylko wybrane osoby. Tworzenie kopii zapasowej danych elektronicznych powinno być wykonywane przez partnera systemu ICT.

Zamykane pojemniki na odpady powinny być stosowane do przechowywania danych w formacie papierowym, które będą utylizowane w sposób gwarantujący bezpieczeństwo danych.