Enervent group

PRIVACY POLICY

Personal Data Act (523/1999) sections 10 and 24

Name of the register
eAir WEB

Purpose of personal data processing
Online portal of the ventilation units' eAir control system

Data collector
Enervent Oy, Kipinätie 1, FI-06150 Porvoo, Finland

Contact person and the data protection officer at the Enervent group
Enervent Oy, Kipinätie 1, FI-06150 Porvoo, Sonja Häggman, tel. +358 20 7528 800, e-mail enervent@enervent.com

Supervisory authority
The data protection officer's office in Finland

Profiling
For the part of personal data, no profiling or automatic individual decisions will be performed.

Data transfer outside the EU or EEA
Data will not be transferred outside the EEA.

Right to check and correct the data and to transfer it to another system
Every person has the right to check and correct their data that has been saved in the person register (for the part of the electronic data provided by the data subject) and to transfer it to another system. Requests: Enervent Oy, Kipinätie 1, FI-06150 Porvoo, Sonja Häggman, tel. +358 20 7528 800, e-mail enervent@enervent.com

Right to be forgotten
Every person has the right to get their personal data removed from the system. Requests: Enervent Oy, Kipinätie 1, FI-06150 Porvoo, Finland
Sonja Häggman, tel. +358 20 7528 800, e-mail enervent@enervent.com

Prerequisite for processing personal data (consent, legitimate interest, agreement, or statutory obligation)
Consent

Special (sensitive) personal data content of the register
None

Ordinary personal data content of the register
The IP address of the ventilation unit and the technical setting, status, and measurement data from the ventilation unit and the connected sensors.

Regular data sources
The data is transmitted from the ventilation unit.

Regular release of data
The data is in an encrypted form in the cloud service of the service provider, and it can only be accessed by the data subject unless they have authorized Enervent Oy to monitor the ventilation unit in question.
The data shall not be released outside the Enervent group or its parent company.

Direct marketing
Personal data shall not be released outside the Enervent group. Enervent may, however, use the data for direct marketing purposes after receiving separate permission.

Data retention time
The data is not intended to be removed from the system, as it contains information that is essential for the maintenance of the delivered ventilation units. The operating life of the ventilation units is decades.

Processes regarding the checking, correction, transfer, and removal of personal data
When a data subject requests the checking, correction, transfer, or removal of personal data, the contact person for the register shall start the corresponding predetermined process. The process includes:
1) Informing the data subject of the reception of the request (within 7 days of receiving the request)
2) Determining the actions to be taken and selecting the persons responsible (within 14 days of receiving the request)
3) Taking the determined actions
4) Documenting the actions
5) Informing the data subject of the actions that have been taken (within 30 days of receiving the request)

Data security violations

If transferred, saved, or otherwise processed personal data is accidentally or illegally destroyed, lost, or edited or if an unauthorized release or access of the data is detected, the administrator of the register shall immediately inform the CEO of this matter. The CEO shall start a process during which

1) Corrective measures shall be taken immediately to avoid further damage
2) The supervisory authority shall be informed of the incident within 72 hours of the detection of the violation in accordance with the instructions of the authority in question
3) The data subjects whom the violation concerns shall be informed of the matter as soon as possible if the violation is likely to pose a great risk to them
4) Improvement measures shall be taken to avoid further data security violations
5) The supervisory authority shall be informed of the actions that have been taken

Register protection principles

Data in electronic format is password-protected, and only selected persons can access it.
Data in paper format is stored in a locked cabinet, to which only selected persons have the key. The backup copying of the electronic data shall be taken care of by an ICT system partner.
Locked waste containers shall be used to store data in paper format, which will be disposed of in a data-secure manner.