

Häufig gestellte Fragen (FAQ) zum Datenschutz bei der intelligenten Heizungssteuerung von vilisto

Inhaltsübersicht

1. Wie funktioniert die intelligente Heizungssteuerung von vilisto?	1
2. Welche Datenschutz-Verantwortung tragen der Kunde und vilisto?.....	2
3. Wie werden die Betroffenen (Mitarbeiter) informiert?.....	2
4. Wie ist der DSGVO konforme Einsatz der Heizungssteuerung sichergestellt?	3
5. Wie kann sichergestellt werden, dass die Daten nicht zur Mitarbeiterüberwachung genutzt werden?	4
6. Wo werden die Daten verarbeitet?	4
7. Wie wird die Datensicherheit gewährleistet?.....	4

1. Wie funktioniert die intelligente Heizungssteuerung von vilisto?

Die vilisto Heizungssteuerung ist ein selbstlernendes System zur Heizungssteuerung bestehend aus Thermostaten und Vor-Ort installierten Steuerungseinheiten („Gateways“). Die Thermostate verfügen über verschiedene Sensoren zur Ermittlung des Raumklimas und zur Erkennung, ob der Raum aktuell oder potenziell genutzt wird. (Bewegungsmelder, Schallpegelsensor, Umgebungslichtsensor, Thermometer und Luftfeuchtigkeitssensor).

Die Daten der Sensoren werden in den Thermostaten vorverarbeitet (z.B. Ermittlung der Überschreitung gewisser Geräuschpegel). Die Ergebnisse werden per verschlüsselter Funkverbindung an das Gateway gesendet. Mithilfe dieser Daten ermittelt das Gateway anhand eines selbstlernenden Algorithmus die Wahrscheinlichkeit, mit der sich aktuell und in der Zukunft) Personen im Raum aufhalten und steuert entsprechend die Wärmeabgabe der Heizkörper, sodass Energie gespart wird, wenn der Raum nicht genutzt wird. Die Wahrscheinlichkeitswerte werden in einer Datei abgespeichert, die fortlaufend aktualisiert wird.

Die Daten werden vom Gateway über eine sichere, verschlüsselte Verbindung zu einem Server übermittelt, dort gespeichert und sind über eine geschützte webbasierte Online-Plattform zugänglich. Über die Online-Plattform können Berechtigte die Thermostate und die Gateways verwalten (z.B. Zuordnung von Thermostaten zu Räumen), Daten visualisieren (z.B. Temperatur, Luftfeuchtigkeit, Batteriestatus) und Heizungseinstellungen vornehmen (z.B. Soll- und Absenkttemperaturen).

2. Welche Datenschutz-Verantwortung tragen der Kunde und vilisto?

Die Daten der Heizungssteuerung beziehen sich auf Thermostate und Räume. Dem Kunden kann es im Einzelfall anhand von Raumbelungsplänen möglich sein, diese Daten einzelnen Personen zuzuordnen (So können beispielsweise über Temperaturverläufe Rückschlüsse auf eine regelmäßige Anwesenheit zu bestimmten Zeiten getroffen werden.). Die vilisto Heizungssteuerung wurde daher so konzipiert, dass sie den Anforderungen der Datenschutzgrundverordnung (DSGVO) und des Bundesdatenschutzgesetzes (BDSG) an den Umgang mit personenbezogenen Daten genügt.

Der Kunde, der die Räumlichkeiten für seine Mitarbeiter bereitstellt, ist „Verantwortlicher“ im Sinne der DSGVO. Die vilisto GmbH betreibt die Online-Plattform und kann im Rahmen von Wartungsarbeiten Zugriff auf Daten der Thermostate und der Gateways haben.

Die vilisto GmbH handelt dabei als Auftragsverarbeiterin nach Art. 28 DSGVO. Das heißt, der Kunde allein bleibt „Herr der Daten“. vilisto nutzen die Daten streng zweck- und weisungsgebunden zur technischen Bereitstellung des Systems.

vilisto bietet den Kunden den Abschluss eines DSGVO konformen Auftragsverarbeitungsvertrags an. Dieser wurde von einem IT-Fachanwalt spezifisch für die vilisto Heizungssteuerung erstellt.

3. Wie werden die Betroffenen (Mitarbeiter) informiert?

Die Pflicht zur Information der Betroffenen gemäß der DSGVO obliegt dem Kunden als datenschutzrechtlich „Verantwortlichen“.

vilisto stellt dem Kunden hierzu kostenlos ein Musterdokument für Datenschutzhinweise bereit. Dieses wurde von einem IT-Fachanwalt speziell für die vilisto Heizungssteuerung erstellt. Mithilfe der Vorlage kann der Kunde seine Informationspflichten nach Art. 12, 13 und 21 DSGVO erfüllen, indem er es betroffenen Mitarbeitern zur Kenntnis gibt, z.B. per E-Mail, Aushang oder Bereitstellung im firmeninternen Intranet.

Die Datenschutzhinweise informieren in verständlicher Form über die erhobenen Daten, deren Nutzung sowie über Rechtsgrundlagen, Speicherfristen und Rechte nach der DSGVO.

4. Wie ist der DSGVO konforme Einsatz der Heizungssteuerung sichergestellt?

Bereits bei der Entwicklung des Systems wurden die Anforderungen der DSGVO identifiziert und berücksichtigt (so genannter „Privacy by Design“ Ansatz). Wichtige Aspekte waren dabei:

Datenminimierung: Die Datenverarbeitung findet weitgehend in den Thermostaten und den Gateways statt, sodass z.B. Rohdaten der Präsenzsensoren nicht in der Online-Plattform gespeichert werden. Historische Daten über die Präsenz einer Person im Raum werden nicht gespeichert. Die aktuell ermittelte Präsenzwahrscheinlichkeit wird nur für die Regelung der Heizung und die Ermittlung der Wahrscheinlichkeit der zukünftigen Raumnutzung verwendet und unverzüglich verworfen.

Speicherbegrenzung: Für alle Daten wurde abhängig vom Nutzungszweck (z.B. Heizungssteuerung, Fehleranalyse) die konkret erforderliche Speicherfrist ermittelt und restriktiv festgelegt. Nach Ablauf definierter Speicherfristen löscht das System die Daten automatisch. Der Kunde kann die vorausgewählten Speicherfristen in der Online-Plattform individuell anpassen und Daten einzelner Thermostate selektiv löschen.

Zugriffsbegrenzung: Der Zugriff auf die Daten erfolgt über die Online-Plattform. Diese verfügt über ein abgestuftes Rollen- und Berechtigungskonzept. So kann sichergestellt werden, dass nur diejenigen Personen Zugriff auf die Daten haben, die diese für ihre konkrete Tätigkeit wirklich benötigen (z.B. Gebäudemanager). Der Kunde kann die Rollen seinen Mitarbeitern intern selbst zuweisen. Um einen Missbrauch zu erschweren gibt es für den Kunden keine Möglichkeit die Präsenzwahrscheinlichkeiten einzusehen. Die Daten stehen lediglich als Rohdaten über die Exportfunktion zur Verfügung.

Betroffenenrechte: Mittels der Online-Plattform können gespeicherte Daten zu Thermostaten exportiert werden. Daten lassen sich zudem selektiv löschen und die Datenerfassung durch einzelne Thermostate kann zeitweise oder dauerhaft deaktiviert werden. Dies dient der Umsetzung von Betroffenenrechten nach der DSGVO (z.B. auf Auskunft, Löschung oder Sperrung).

Ein komplexes technisches System wie die vilisto Heizungssteuerung muss notwendigerweise eine Reihe von Daten erfassen, ähnlich wie andere Systeme, etwa Betriebssysteme von Computern, Smartphones oder Software in PKWs. Durch die beschriebenen Maßnahmen wird jedoch sichergestellt, dass das Risiko eines Missbrauchs von Daten (z.B. unzulässige Mitarbeiterüberwachung) minimiert ist.

5. Wie kann sichergestellt werden, dass die Daten nicht zur Mitarbeiterüberwachung genutzt werden?

Wie unter 4. beschrieben verarbeitet vilisto die Daten zweckgebunden für die Steuerung der Heizkörper und stellt die Daten „DSGVO-konform“ zur Verfügung, so dass ein Missbrauch für andere Zwecke erschwert ist. Die Zweckbestimmung der Daten obliegt jedoch allein dem Kunden. Durch folgende zusätzliche Maßnahmen kann die Nutzung für Zwecke der Leistungs- und Verhaltenskontrolle durch den Kunden explizit ausgeschlossen werden:

- Betriebsvereinbarung
- Festlegung der Zwecke im internen Verzeichnis der Verarbeitungstätigkeiten nach Art. 30 DSGVO
- Erläuterung der Zwecke in den Datenschutzhinweisen nach Art. 13 DSGVO.

6. Wo werden die Daten verarbeitet?

Die Datenverarbeitung erfolgt ausschließlich vor Ort in den Thermostaten und Gateways und in dem für die Online-Plattform genutzten Rechenzentrum. Dieses befindet sich derzeit in Deutschland. Eine Übermittlung in Länder außerhalb der EU findet nicht statt.

7. Wie wird die Datensicherheit gewährleistet?

vilisto hat geeignete Maßnahmen getroffen, um die Daten vor dem Zugriff durch Unberechtigte zu schützen.

So werden die Daten von den Thermostaten bis zum Server ausschließlich verschlüsselt übertragen. Die Daten werden in sicheren Rechenzentren in Deutschland gespeichert. Die Online-Plattform ist ausschließlich über eine verschlüsselte Verbindung und mit Authentifizierung erreichbar.

Alle Maßnahmen zur Datensicherheit sind für den Kunden detailliert in dem Dokument „Technische und Organisatorische Maßnahmen“ zusammengestellt.