Privacy statement
SaaS Hoval Cloud systems

1. Privacy information for the use of SaaS offerings

This privacy information applies to the SaaS offerings of Hoval Cloud systems (HovalSupervisor cloud and HovalConnect) of Hoval AG (referred to below as “Hoval” or “we”). HovalConnect includes the mobile application for system owners and other system users (“HovalConnect App”) as well as the business application provided to Hoval partners (“HovalConnect business”). It explains how your personal data is collected, processed, and used when you use Hoval Cloud systems.

With regard to SaaS offerings provided by Hoval Cloud systems, reference is made to joint data processing via the respective online portal, if one exists. Joint data processing is carried out in accordance with the terms of use and the privacy statement of the respective online portal.

As the controller, we take the protection of your personal data very seriously. We treat your personal data confidentially and in accordance with Swiss, EU and UK laws governing data protection and this privacy information. We also ensure appropriate and secure processing and apply appropriate measures to protect and maintain the confidentiality, integrity and availability of your data. Our security measures are continuously improved to reflect the latest technological developments.

This privacy policy information contains more detailed information about:

- Contact information of the data controller
- Categories of data processed
- Information on the purpose and legal basis
- Data recipient
- Storage duration
- Information about your rights

2. Who are we?

The data controller is Hoval AG with its headquarters in Vaduz, Liechtenstein, and the companies assigned to it. An overview of the companies belonging to the Group can be found at www.hoval.com.

If you have any questions about the privacy policy, please contact our data protection officer by e-mail at dpo@hoval.com.

3. Who is responsible for your data

Depending on how your system was connected, Hoval is responsible for your data either on its own or jointly with another company:

Your situation	Responsible
You are using HovalConnect.	Hoval
You are using HovalConnect business	Hoval and you, as a Hoval partner/system administrator, jointly (Article 26 of the GDPR)
Your system was connected to the HovalSupervisor cloud directly by Hoval.	Hoval

Privacy statement
SaaS Hoval Cloud systems

Your situation	Responsible
Your system was connected to the HovalSupervisor cloud by your provider or system administrator.	Hoval and your provider or system administrator jointly (Article 26 of the GDPR)

a) Sole responsibility
For HovalConnect and HovalSupervisor cloud with direct connection by Hoval, Hoval is the sole data controller in the sense of Article 4(7) of the GDPR or, to the extent that the data protection law of the United Kingdom applies, Article 4(7) of the UK GDPR. There is no joint responsibility under Article 26 of the GDPR or Article 26 of the UK GDPR with respect to these services. A professional customer is not involved in the processing as a data controller.

b) Joint responsibility
For HovalConnect business and HovalSupervisor cloud, Hoval and the professional customer are joint data controllers in the sense of Article 26 of the GDPR or, to the extent that the data protection law of the United Kingdom applies, Article 26 of the UK GDPR, provided that the processing in question is carried out jointly by Hoval and the professional customer. In the case of HovalSupervisor cloud, this applies in particular when the end customer's system was activated by a professional customer.

The parties have entered into a joint responsibility agreement that specifies which of them is responsible for fulfilling which obligations under the applicable data protection laws.

Hoval coordinates the processing of incoming inquiries in order to simplify the process. Inquiries should preferably be directed to Hoval's Data Protection Officer at dpo@hoval.com.

With regard to data processing, Hoval assumes the following responsibility:

- for the collection of data
- for the storage of data
- for the modification and deletion of the data, the restriction of data processing and data transfer
- for appropriate security of data transfer and processing.
- for compliance with the statutory retention obligations in relation to the data
- for compliance with nationally applicable data protection regulations and requirements
- for the confidential handling of data and appropriate processing of data

With regard to data processing, the customer assumes the following responsibility, unless it is the end customer:

- for establishing an agreement with the end customer that complies with data protection regulations, in particular an appropriate legal basis for the collection, processing, and use of the customer's personal data
- for enabling access to the end customer's own data in compliance with data protection regulations, for example by creating a new user profile for the end customer
- for enabling an end customer to switch to a data processing service in accordance with section 7 of this privacy statement

Hoval and the professional customer shall support one another in responding to requests from data subjects and in complying with statutory data protection obligations; in doing so, each party shall perform the tasks that it is better able to perform or is solely responsible for performing under this statement and applicable laws.

c) Processors
Both Hoval and the professional customer may engage service providers as processors within the meaning of Article 28 of the GDPR – or, to the extent that the data protection law of the United Kingdom applies, Article 28 of the UK GDPR – for the processing activities for which they are respectively responsible.

Each party shall ensure that a data processing agreement is entered into with its processors in accordance with Article 28 of the GDPR or Article 28 of the UK GDPR, and that the requirements of the applicable data protection laws are met.

To the extent necessary to fulfil their joint obligations under the joint responsibility arrangement, the parties shall inform one another of the processors they have engaged.

4. What information do we collect about you?

We process personal and non-personal data (collectively, “Data”) that is generated in connection with the use of our SaaS offerings and cloud services.

The personal data recorded includes, depending on which SaaS Hoval Cloud system is used in each case (this is not an exhaustive list):

- Customer master data (name, address, contact data)
- Contract data (customer number, services booked, payment information)
- Service data
- User, access, and connection data
- User roles and access permissions
- Project and system IDs
- Alarm and event data
- Log data regarding user accesses as well as parameter and configuration changes

Technical and system-related data (this is not an exhaustive list):

- System, operational, and configuration data resulting from the use of cloud services and other services
- System and measurement data, particularly temperatures, outputs, flow rates, and meter readings
- Output and utilization data
- Fault and safety reports
- Technical data on units and operating systems
- Data for optimizing, monitoring and further developing the services

5. Purpose of processing

We process your data solely to provide and operate our SaaS services and cloud platforms, to fulfil contracts, to bill you, and to provide customer support (for example, by contacting you or scheduling appointments, including maintenance, optimisation, and monitoring, as well as remote technical support and maintenance provided directly by Hoval, to the extent that this is part of the agreed service or has been agreed separately). Furthermore, the processing of personal data serves to ensure IT security, prevent misuse and ensure the operational reliability of our systems, as well as to enable the continuous improvement, monitoring and further development of our software, and to fulfil our legal obligations. Lastly, we will assist

you in switching to other data processing services by exporting your data in accordance with the EU Data Act.

6. Legal basis

We always process personal data solely on one of the legal bases set out in Article 6(1) of the GDPR or, to the extent that the data protection law of the United Kingdom applies, Article 6(1) of the UK GDPR. The allocation to the respective purposes is carried out as follows:

- Provision and operation of SaaS and cloud services: processing for the purposes of fulfilling the contract or taking steps prior to entering into a contract (Article 6(1)(b) of the GDPR or the UK GDPR).
- Billing, contract management and payment processing: contract performance (Article 6(1)(b) of the GDPR or the UK GDPR).
- Maintenance, support, optimisation and monitoring of the customer system (subject to a separate contract): contract performance (Article 6(1)(b) of the GDPR or the UK GDPR).
- Direct connection of a system to the HovalSupervisor cloud by Hoval, insofar as this is necessary for the provision of the agreed cloud or remote support service: contract performance or the implementation of pre-contractual measures (Article 6(1)(b) of the GDPR or the UK GDPR).
- Remote maintenance of a system directly connected by Hoval: legitimate interest in the trouble-free, safe and energy-efficient operation of the system (Article 6(1)(f) of the GDPR or the UK GDPR). You may object to this processing in accordance with Article 21 of the GDPR or the UK GDPR.
- Customer communications and service enquiries (e.g. support, arranging appointments): legitimate interest in providing efficient and secure customer service (Article 6(1)(f) of the GDPR or UK GDPR).
- IT and operational security, functional security, prevention of misuse: legitimate interest in maintaining secure systems (Article 6(1)(f) of the GDPR or the UK GDPR).
- Continuous improvement, monitoring and further development of our software: legitimate interest in the optimisation and further development of our software and services (Article 6(1)(f) of the GDPR or the UK GDPR).
- Compliance with legal obligations, in particular commercial and tax law retention requirements: legal obligation (Article 6(1)(c) of the GDPR or the UK GDPR).
- Marketing and information activities: processing with your consent, where such consent is required under the applicable data protection and direct marketing regulations (Article 6(1)(a) of the GDPR or the UK GDPR).

Non-personal data is not subject to the GDPR or the UK GDPR. Your data will be processed and used in accordance with the relevant statutory provisions, in particular the EU Data Act, insofar as it applies, and this privacy information, to the extent that this is necessary for the performance of the contract or the provision of services, or is otherwise permitted by law.

7. Obligations under Chapter VI of the EU Data Act relating to data processing

As a provider of data processing services, particularly SaaS services, we make it possible to switch to another data processing service or return to an in-house solution. You have the right to receive the data we hold about you in a structured, commonly used and machine-readable format. We ensure that data export is technically feasible and provide transparent information on procedures, timeframes, formats and any costs involved. Interoperability shall be ensured insofar as this is technically feasible and legally permissible. No unfair barriers will be created to prevent consumers from switching providers.

Should you wish to switch to another data processing service, please notify us in writing.

The transition period for changing data processing services is, as a rule, 30 calendar days from the end of the notice period. If the 30-day transition period for the switch is not technically feasible, we will inform you of this within 14 working days of your application and specify alternative transition periods, which will not exceed 7 months.

In addition, the provisions of Chapter VI of the EU Data Act apply, in particular Article 25 of the EU Data Act.

8. Data retention

We process and store your personal data for the duration of the relevant contractual relationship.

Upon termination of the contractual relationship, including in the event of a change of data processing service, we will delete the exportable data and digital assets generated by you or directly attributable to you, provided that there are no statutory retention obligations to the contrary.

The data will be deleted as soon as it is no longer required for the purposes of contract fulfilment, or at the latest 12 months after the end of the contract.

In accordance with commercial and tax law, we retain invoices, payment details and contracts for ten years from the end of the relevant financial year. During this period, we process this data solely for the purpose of complying with our retention obligations and delete it afterwards.

We store system and measurement data in a time-series database, which is technically necessary for the applications you use. Furthermore, these records are retained for analytical purposes. The readings can be linked to you provided you have registered your system as the owner in HovalConnect. If your user account is deleted, this association will be removed; any names you have assigned, such as the asset name, will be reset to the serial number. The system and measurement data are then stored anonymously and are only used for the operation and further development of our services.

We will delete your user account once the transition period for changing the data processing service, as set out in clause 7, has expired, or at the latest 60 days after the end of the contract. You may also request that your data be deleted at any time.

Data may be stored for a longer period where this is necessary to comply with retention obligations under EU law, to safeguard legitimate interests, or to establish, exercise or defend legal claims. In such cases, the data will be deleted once the relevant purpose no longer applies.

9. Disclosure of data

We only disclose personal data where there is a legal basis for doing so. This may be the case, in particular, if you have given your consent, if the disclosure is necessary for contract performance, if there is a legal obligation, or if the disclosure is permitted in order to safeguard legitimate interests.

Where an end customer grants a Hoval partner access to their system via HovalConnect Business, the authorised Hoval partner will be granted access to the data intended for the authorised system access, to the extent permitted by the relevant access authorisation. Insofar

as the Hoval partner processes this data for its own service, maintenance or support purposes, it is independently responsible for this processing under data protection law.

In addition, we may use service providers who process personal data on our behalf, for example for hosting, IT operations or support. These service providers are contractually bound to comply with the applicable data protection requirements.

To the extent that the EU Data Act applies, we will, at the user's request, make data available to a third party designated by the user, provided that the legal requirements for doing so are met.

10. Disclosure to public authorities and compliance with legal obligations

In certain circumstances, we may be legally obliged to disclose personal data to public authorities, courts or other public bodies. In this case, we will only disclose the data to the extent necessary to fulfil our legal obligations.

11. Data transmission to third countries

Where we transmit personal data to countries outside the European Economic Area or have it processed there, this is done in accordance with the requirements set out in Articles 44 et seq. of the GDPR. Data will be transferred, in particular, on the basis of an adequacy decision by the European Commission or appropriate safeguards, in particular recognised standard contractual clauses, provided that the legal requirements for this are met.
To the extent that the UK GDPR applies and personal data is transmitted from the United Kingdom to another country or made available there, the transmission shall be carried out in accordance with the relevant provisions of the UK GDPR. In this regard, particular use may be made of UK adequacy arrangements, appropriate safeguards or a statutory exemption.

12. Liability

In the event of breaches of the applicable data protection regulations, the statutory liability provisions shall apply, in particular Article 82 of the GDPR or, to the extent that the data protection law of the United Kingdom applies, Article 82 of the UK GDPR.

13. Advertising and marketing

If you have given your consent, we will process your personal data for marketing purposes. This includes information on new services, service offerings and selected cooperation partners. The legal basis is Article 6(1)(a) of the GDPR or, where applicable, Article 6(1)(a) of the UK GDPR. You can withdraw your consent at any time with effect for the future. Where we engage service providers to carry out marketing activities, their engagement is governed by the applicable data protection requirements.

14. Security

We protect your personal data through appropriate technical and organisational measures in accordance with Article 32 of the GDPR or Article 32 of the UK GDPR, where applicable. Security is an integral part of the development and operation of our systems.

In particular, we are implementing the following measures:

Technical measures:

- Encrypted data transmission between systems and cloud infrastructure in accordance with recognised security standards
- Logical client isolation to prevent unauthorised access between client instances.
- Encrypted storage of customer data.

- Ongoing monitoring of systems to detect security incidents and anomalies.

Organisational measures:

- Regular security audits, including external penetration tests
- Internal processes for implementing statutory requirements such as NIS 2, the Cyber Resilience Act and the EU Data Act.
- Preparation and further development with regard to recognised safety standards, in particular IEC 62443-4-2.

15. What rights do you have?

a) Rights under data protection law

Where we process your personal data, you are entitled to the following rights in particular, in accordance with the applicable data protection regulations:

- Right to information about your personal data
- Right to have inaccurate personal data rectified or incomplete personal data completed
- Right to deletion of your personal data
- Right to restriction of processing
- Right to data portability
- Right to object to certain forms of processing
- Right to withdraw consent that has been given, with effect for the future

To exercise your rights or if you have any questions regarding the processing of your personal data, please contact our Data Protection Officer at dpo@hoval.com.

b) Rights under the EU Data Act

To the extent that the EU Data Act applies to the use of our services, you are entitled to the rights set out therein regarding access to and use of data generated whilst using connected products or connected services.

Where required by law, we will provide you with this data, together with the information necessary for its use, in a structured, commonly used and machine-readable format.

If the service you use is classified as a data processing service within the meaning of the EU Data Act, you may also have statutory rights to switch to another provider or to use your own infrastructure. In this case, we will support the transfer in accordance with the applicable legal requirements.

c) Right to complain

You have the right to lodge a complaint with a competent data protection supervisory authority. In the case of Hoval, you may contact the Liechtenstein Data Protection Authority in particular. Where the UK GDPR applies, you may also contact the Information Commissioner's Office (ICO) in the United Kingdom.

Liechtensteinische Datenschutzstelle
Kirchstrasse 8
Postfach 684
9490 Vaduz
www.datenschutzstelle.li

Information Commissioner's Office (ICO)
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF
United Kingdom
www.ico.org.uk

16. Amendments to the privacy statement

If we are obliged to amend this privacy policy information due to modified services or legal requirements, the latest available version shall apply.

Last amended on 22 September 2026