Information on collection of personal data according to the GDPR for customers

The EU General Data Protection Regulation requires us to provide you with comprehensive information for processing of your personal data. In compliance with this obligation, we inform you of the following:

I. Processor

1.1 Name and contact details of the controller

SmartHeat Deutschland GmbH, Am Augraben 10, 18273 Güstrow
Tel.: +49 3843 22790
Fax: +49 3843 683132
eMail: info@smartheat.de

1.2 Name and contact details of the representative in the EU according to sect. 27 GDPR
(only if the controller or processor is not resident in the Union)

not applicable

1.3 Contact details of the data protection officer

External data protection officer:
ECOVIS Grieger Mallison Rechtsanwälte PartG mbB
Axel Keller (lawyer) / Susann Harder (lawyer)
Am Campus 1 – 11, D-18182 Rostock-Bentwisch
Phone: 0381 – 649 210 Email: dsb-nord@ecovis.com
Web: www.ecovis.com/datenschutzberater

II. Processing scope

2.1 Categories of personal data concerned that are processed
In the scope of our business relationship and depending on the specific purpose for which we collect your data, we regularly process the following data or categories of data:
General:
Address data
Contact data
Bank information
Personal data
Public, electronic and financial identification data
Earnings/income
Spendings/debt
Special income
Credits
Insurances
Pensions
Financial transactions
Professional work
Agreements/conventions
Patents/licenses
Immigration status
Physical details
Habits
Lifestyle
Details regarding travels/trips
Social contacts
Property
Public mandates performed
Complaints/incidents
Accidents
Personality/character
Marriage-partnerships
Marriage chronology
Family/household members
Free-time activities/interests
Memberships
Service provider
Service recipient
Residential address
Physical health condition
Mental health condition
Risk characteristics
Genetic data
Medication data
Publications
Financing of trainings
Current workplace
Ethnic data
Sexual behaviour
Image recording data
Sound recording data

2.2 Source of personal data

We generally collect your data in direct contact with the data subject. However, it is also possible that you may submit data on persons who are responsible for us in your company to us.

2.3 Duration of storage of the data

The personal data collected by us will be stored according to the proviso of our erasure concept until the end of the statutory archiving obligation; they will then be erased, except of we are obligated to archive the data for a longer period according to section 6 para. 1 s. 1 lit. c GDPR due to archiving and documentation obligations under tax and commercial law (from the Commercial Code, Criminal Code or Tax Code) or if you have consented to storage beyond this according to sect. 6 para. 1 s. 1 lit. a GDPR.
Subject to such archiving obligations, data are deleted if the purpose for which they were collected has ended.
As far as legally permitted, data will also be stored if this is required to assert or defend any legal claims.

2.4 Purposes of processing

The purposes of processing of your data are

- processing of a business relationship between us, including communication between us, in particular for processing of the payment transactions, accounting and performance of the contractual obligations between us.

2.5 Legal basis for processing

We only process your data if there is a legal basis for it. This is the case according to sect. 6 para. 1 GDPR when at least one of the following provisions is met.

a. processing is necessary for the **performance of a contract** to which you are a party or in order to **take steps** at your request **prior to entering into a contract**;
b. processing is necessary for **compliance with a legal obligation** to which we are subject;
c. processing is necessary to **maintain our legitimate interests** except where such interests are overridden by your interests or fundamental rights and freedoms which require protection of personal data.

2.6 Legitimate interests within the meaning of sect. 6 para. 1 lit. f GDPR

Our legitimate interests – or those of a third party – may be

a. the presence of a legal relationship between us;
b. the prevention of fraud;
c. measures to ensure and improve the safety of IT systems;
d. measures to protect our company from illegal actions and
e. internal administrative purposes, in particular exchange of data within our group of companies.

2.7 Legal or contractual obligation to provide the data

An obligation to provide data may result

a. from a contract you have concluded with us and the performance of which data collection serves in the cases of item 2.5 lit. b;
b. from the statutory provisions we are subject to or – in accordance with sect. 6 para. 2 and 3 GDPR – the law of the European Union or the law of the member states of the European Union in the cases of item 2.5 lit. c.;
c. from general support or contractual secondary obligations that are not specifically targeted at data collection, such as the provisions on failure to render assistance in § 323c Criminal Code, in the cases of items 2.5 lit. d. and e.

2.8 Requirement of the provision of data for conclusion of a contract

The data collected by us are usually mandatory for founding and processing of a business relationship, including meeting the obligations resulting from this.

2.9 Other obligation to provide the data

There usually is no other obligation to provide the data.

2.10 Possible consequences of not providing data

Not providing personal data of persons working for your company usually only causes makes communication between us considerably more difficult or impossible - e.g.in the area of communication by email.

2.11 Presence of automated decision-making (including profiling)

We do not use any automated supervision or evaluate systems.

III. Forwarding and other countries

3.1 Recipients or categories of recipients of the personal data

The data collected by us will be forwarded to other recipients and third parties as well under consideration of the statutory provisions. These specifically are:

Internal recipients:	External recipients:
- Business management	- Tax advisor
- Accounting / book-keeping	- Financial administration
- Purchase / procurement	- Lawyer
- Department manager	- External data processors (contract processors)

External data processors may be from the areas of archive, maintenance and care for EDP systems or the company website or marketing. These usually are contract processors within the meaning of sect. 4 no. 10 GDPR, so that processing of the data through them does not constitute transmission within the meaning of sect. 4 no. 2 GDPR.

3.2 Intention of the controller to transmit personal data to a third country or an international organisation

Such transmission is not intended.

3.3 Presence or absence of a commission decision on appropriateness

Not applicable.

3.4 Reference to suitable or appropriate safeguards

Not applicable.

IV. Your rights

4.1 You as the data subject have various rights under the General Data Protection Regulation. These are

- the right to be informed about the data concerning you that are stored by us (sect. 15 GDPR)
- the right to rectification of incorrect data (sect. 16 GDPR)
- the right to erasure of the data if there is no legal basis for continued storage (sect. 17 GDPR)
- the right to restriction of processing of the data to specific purposes (sect. 18 GDPR)
- the right to data portability (sect. 20 GDPR) and
- the right to object to processing of your data (sect. 21 GDPR).

If processing of your data is based on consent (see item 2.5 lit. a), you have the right to withdraw your given consent at any time. The legality of the processing taking place based on given consent until the withdrawal is not affected by the withdrawal.

Separate information about the right to object under Article 21 GDPR

According to Article 21 (1) of the GDPR, you have the right at any time, for reasons arising from your particular situation, to object to the processing of personal data re-lating to you pursuant to Article 6 (1) (f) of the GDPR (processing to safeguard the le-gitimate interests of the responsible entity or a third party).

If you object, we will no longer process your personal data, unless we can demon-strate compelling legitimate grounds for processing that outweigh your interests, rights and freedoms, or the processing is for the purpose of asserting, exercising or defence of legal claims.

If the processing is to operate direct mail, you have the right, under Article 21 (2) GDPR, to object at any time to the processing of personal data relating thereto for the purpose of such advertising; this also applies to the profiling, as far as it is associated with such direct mail.

In addition to this, you have the right to complain to a supervisory authority in accordance with sect. 77 GDPR if you believe that processing of the data concerning you violates provisions under data protection law. The supervisory authority relevant for us is:

The State Data Protection and Freedom-of-Information Officer
Mecklenburg-Vorpommern
Schloss Schwerin, Lennéstraße 1,
19053 Schwerin
Phone: +49 385 59494 0
Fax: +49 385 59494 58
eMail: info@datenschutz-mv.de
web: www.datenschutz-mv.de; www.informationsfreiheit-mv.de
https://www.datenschutz-mv.de/kontakt/kontaktformular/

4.2 Finally, you have the right to contact our data protection officer at any time. He is obligated to confidentiality regarding your query where processing of your data is concerned.

You can reach our data protection officer under the contact details named in item 1.3.

Date of publication 17th August 2020: Update of our privacy policy: On the basis of the decision of the European Court of Justice of 16th of July 2020, we hereby inform our customers, business partners, employees, website visitors and other communication partners that it may not be possible to maintain an adequate level of data protection comparable to that required by EU regulations when using US service providers such as Amazon, Asana, Facebook, Google, MailChimp, Twitter, TeamViewer, YouTube, etc. and their respective european subsidiaries within the scope of communication. Due to national laws, a non-european provider may be forced by national law to surrender communication data to national security authorities without the possibility of such surrender being reviewed for its legality in an independent judicial procedure at the request of the data subject. Since this finding of the court also applies to companies based and processing data in Europe under the so-called EU-US Privacy Shield, as well as the Standard Contractual Clauses and the Binding Corporate Rules, we must now examine all data transfers to third-party providers on a case-by-case basis and, if necessary, discontinue them or replace them with EU-based providers. We are currently in discussions with our service providers and the supervisory authorities.