

Agreement on the provision of product data (EU Data Act)

between

RESOL – Elektronische Regelungen GmbH

Heiskampstr. 10, 45527 Hattingen, Germany

– hereinafter referred to as the "data holder" –

and

any party that identifies themselves as a user within the meaning of Regulation (EU) 2023/2854 (hereinafter referred to as the "EU Data Act") and declares their express or implied (final) agreement with the terms of this data usage agreement, e.g. during a registration process to create a personal user account for use of the related service(s), when extending the functionality of the related service(s) by subscriptions, or when engaging additional services (e.g. maintenance or monitoring) that require the use of the data collected under this data usage agreement.

– hereinafter referred to as the "user" –

1. Subject

The data holder shall provide the user with certain data that is generated or logged when purchasing or using the following networked products:

1.1 Networked products

- All solar, heating, DHW exchange and multifunction controllers except the DeltaSol® A/AX/AX HE
- All controllers for heat transfer, biomass and power-to-heat
- All controllers installed in the pump stations
- KM2 communication module and DL2 Plus datalogger
- Calorimeter WMZ Plus

1.2 Related services

- RESOL RSC service centre software
- VBus.net and RPT parameterisation tool
- RESOL apps from the VBus®Touch family

The agreement exclusively governs the provision and use of the data specified in this agreement.

2. Categories and provision of data

The data holder shall provide the user with the readily available data (raw data and pre-processed data as defined by the EU Data Act) generated during use of the product via the following interfaces:

1) Local data logging via SD card

Logging takes place directly in the product. Access is offline by the user physically reading the SD card. The data is only available as a CSV file in this way.

2) Local data logging in the datalogger

For the purpose of data logging, the product requires the connection of the DL2 Plus datalogger to the VBus® interface. Data access and visualisation can take place continuously on the local network without a user account using the RESOL RSC service centre software, the VBus®Touch app family or, if available, via the web interface integrated into the device.

3) Local data logging on a PC

The RSC service centre software continuously stores the product data on the PC. The transfer takes place in the local network without a user account via the interface adapter VBus®/USB, which is connected to the product via VBus®.

4) Server-side data logging

The data is continuously transmitted to our servers via the DL2 Plus datalogger or KM2 communication module. Access takes place online via our password-protected web portal VBus.net, which requires a registered user account. In addition to data visualisation and CSV export, the optional RPT IN VBus.net parameterisation tool also enables convenient remote configuration of the product.

The data holder shall always provide the data in the quality and with the latency identical to that in which it is available to the data holder. A guarantee that the data is complete, error-free or available beyond the contractual agreements is not provided.

Scope of data provided:

The data covered by this data usage agreement includes all readily available product data and data generated in connection with related services.

Data of the networked products:

- Operating and usage data: Operating states, error messages, utilisation levels and maintenance events
- Measured values Technical parameters such as temperature, pressure, output, flow rate and runtimes
- Consumption data: Energy consumption and efficiency values
- Metadata: Time stamps and contextual data of the data logging

Data of related services:

- Configuration data: Language, units, date format
- The timestamp of the last login and the number of logins
- Visualisation data: Charts, live systems

Usage logs will not be created.

The actual amount of data varies depending on the intensity of use, the service life and configuration of the product, as well as the intervals for data storage and updates selected by the user.

Estimated data volumes range from 0.15 MB to a maximum of 6.8 MB per day.

Not provided:

- Personal data, unless there is an effective legal basis in accordance with the GDPR
- Data of other users or other products
- Data that is the result of an independent, in-depth analysis or the data-based insights of the data holder (inference data) and does not constitute raw or pre-processed product data.

Specifications for provision:

- Data format: Depending on the type of data logging, either as CSV (all data logging options) or in JSON format via a REST API (data logging option 4 only).
- Up-to-datedness: The data in the product is continuously generated during operation. Data logging options 2, 3, and 4 are essentially delivered in real time, subject to technical configuration.
- Update frequency: The transfer and update intervals can be set manually in the device.
- Location: Servers in a certified European data centre (applies to data logging option 4).

- Retention period: The data shall be stored on the servers of the data holder for the duration of the service period defined in the main contract after its generation and then automatically deleted (applies to data recording option 4).
- Deletion of data: As a user, you have the right to have the data stored about you or your networked product deleted (in accordance with the legal requirements of the GDPR and the EU Data Act). We have integrated a corresponding deletion function into our networked products and related services.

The data specification and the device-specific equipment scope are described in **Appendix A** of this agreement.

3. Purpose and limits of data use

The user is entitled to use the data provided for the following purposes:

- Condition monitoring of the system
- Detection of maintenance requirements
- Preparation of efficiency and utilisation analyses
- Creation of reports for the user

In accordance with **Art. 4 para. 4 and Art. 6 (2) (e)** of the EU Data Act, the user is strictly prohibited from using the data received for the purpose of developing a product or related service that competes with the networked product or related services of the data holder. It is also prohibited to pass on the data to third parties for this purpose or to enable third parties to further develop the data. Any use of the data that goes beyond the permitted purposes mentioned above – in particular for the development of competing products or services – requires the prior, explicit and written consent of the data holder.

Furthermore, the user undertakes not to disclose or violate any business secrets of the data holder when using the data (section 6 additionally applies).

Insofar as the data holder uses the generated non-personal data for their own purposes (e.g. for general product optimisation, warranty claims or further development of their own connected services), they are obliged in accordance with **Art. 4 para. 6** of the EU Data Act, not to use this data to gain insights into the economic situation, operation or business methods of the user, provided that this is done for purposes that compete with the user.

4. Disclosure to third parties

Disclosure to others by the data holder

The data holder is entitled to disclose the non-personal data to third parties (in particular affiliated companies, IT service providers or subcontractors) insofar as this is necessary for the fulfilment of this contract, maintenance of the product, product safety or provision of the connected services. The data holder shall ensure that such third parties are contractually bound by appropriate confidentiality and data security standards. Disclosure of the data to uninvolved third parties for promotional or sales purposes is excluded without the express consent of the user.

Disclosure to a third party designated by the user

At the request of the user, the data holder shall transmit the readily available product data to a third party (data recipient) designated by the user in accordance with the provisions of the EU Data Act. The following conditions apply to this disclosure:

- Obligations of the third party:

The user shall ensure that the designated third party is responsible for all obligations set out in Art. 6 of the EU Data Act. In particular, the third party is prohibited from using the data for the development of a competing product or service, from unauthorised forwarding of the data to other third parties or from forming profiles from it.

- Prior agreement regarding business secrets:

In accordance with Art. 5 para. 9 of the EU Data Act, the data holder is only obliged to transfer data to the third party if an explicit agreement has been concluded between the data holder and the third party regarding technical and organisational measures (TOMs) to protect the data holder's business secrets.

- **Refusal and suspension:**

The data holder reserves the right to refuse, restrict or suspend the transfer of data to the third party if the third party fails to implement the agreed protective measures, if there are reasonable doubts about the protection of business secrets or if the third party demonstrably violates the provisions of the EU Data Act. In this case, the data holder shall immediately notify the competent authority (per Art. 37 of the EU Data Act) that they have refused or suspended the disclosure to others, specifying those measures that have not been agreed or that have not been implemented (Art. 5 para. 10, 11 EU Data Act).

- **Remuneration:**

In return for the provision of the data to the third party, the data holder may receive appropriate and fair remuneration from the third party in accordance with Art. 9 of the EU Data Act (section 8 additionally applies).

- **Exclusion of gatekeepers:**

Disclosure to companies approved by the European Commission per Art. 3 of Regulation (EU) 2022/1925 (Digital Markets Act) as "gatekeepers" as set out in Art. 5 para. 3 of the EU Data Act is excluded. Such companies shall not be considered as approved third parties within the meaning of this agreement.

5. Personal data

Insofar as the data generated, transferred or provided within the scope of this agreement is personal data within the meaning of Art. 4 No. 1 GDPR, the parties undertake to strictly comply with the provisions of the General Data Protection Regulation (GDPR) and the Federal Data Protection Act (BDSG)

If necessary, the parties shall separately determine whether the data recipient (user or a third party designated by the user) is responsible for the respective data processing as an independent controller or jointly responsible controller (Art. 26 GDPR), or as a data processor. To the extent required by law, the parties shall immediately conclude a separate agreement for order processing (AVV) in accordance with Art. 28 GDPR or an agreement defining joint responsibility.

Personal data will be strictly assigned by the parties and processed only to the extent strictly necessary for the agreed purpose (principle of data minimisation). The processing of personal data by the data holder for their own purposes or the provision of such data to the user shall only take place if and insofar as an effective legal basis for this is shown to exist in accordance with Art. 6 para. 1 GDPR.

6. Protection of business secrets and data security

Technical and organisational security

The security of the systems and the data generated is a top priority for the data holder. In order to protect user data and the data holder's own systems, the data holder uses appropriate technical and organisational measures (TOMs) that correspond to the state of the art. This includes, in particular, encrypted data transmission (e.g. for logging on a server), role-based access controls and the security of user accesses through multi-factor authentication.

Preservation of business secrets

The data provided is usually raw technical data or pre-processed data. However, the structure, metadata, configuration parameters, and the specific composition of the data may contain proprietary business secrets of the data owner. Data access and data transmission to the user or a third party designated by the user are subject to the legal proviso that the confidentiality of these business secrets is fully safeguarded. The data holder is entitled to make the provision of the data subject to the prior agreement of specific technical or contractual protective measures (e.g. the conclusion of a confidentiality agreement / NDA, the use of specific encryption methods or restrictions on the disclosure of data) by the user or the designated third party. The user shall ensure that their employees and subcontractors also comply with these obligations.

Legitimate refusal and suspension

In exceptional cases where, despite the agreed protective measures, the disclosure of data would demonstrably lead to serious, irreparable economic damage to the data holder (e.g. due to the threat of disclosure of key development secrets or cyber security risks), the data holder may refuse or suspend the provision of data in a legally permissible manner.

In this case, the following legal procedure shall apply:

- The data holder shall immediately inform the user of the reasons for the refusal or suspension in writing.
- The data holder shall immediately report the decision and the justification to the competent national authority in accordance with the requirements of the EU Data Act.

Security incidents

If, despite the implementation of security measures, a relevant security incident, breach of the protection of business secrets or an unauthorised outflow of data should occur, the parties shall inform each other immediately in order to initiate joint countermeasures.

7. Rights to data and results

This agreement does not transfer ownership rights to the data holder's generated data, product, software or business secrets.

The user is granted a simple right to use the data provided, limited to the purpose of this contract. The user may generate analyses and reports derived from the data for the agreed purpose. Raw data and pre-processed data may not be used outside the purpose agreed in section 3.

8. Remuneration

The data holder shall provide the user with readily available data (raw and pre-processed data) free of charge for the purposes set out in this agreement.

CSV/JSON exports are already included in the free VBus.net basic version.

As a minimum, the data shall be provided in the same quality as it is available to the data holder and in a structured, common and machine-readable format.

Insofar as the user requests the provision of data to a third party, the data holder is entitled to receive appropriate and fair remuneration from this third party (in accordance with Art. 9 of the EU Data Act) for the technical workload and provision.

Any collection of costs or remuneration shall be carried out exclusively within the scope of the applicable legal requirements. The user shall be informed in advance of any costs incurred (e.g. for exceptional special formats or additional transmission channels) in a transparent and comprehensible manner.

9. Contract term and termination

This data usage agreement shall become effective with the express or implied consent of the user (e.g. as part of the registration process to create a personal user account or when engaging related services). The free VBus.net basic version is provided for an indefinite period of time and can be duly terminated by both parties. A fixed term of 12 months applies to the chargeable VBus.net-PRO access. On request, direct booking for several years with a correspondingly longer fixed term is also possible. The PRO agreement ends automatically when the respective selected term expires, without the need for separate termination. Reactivation is then possible at the current fee. When PRO access expires, the user account is automatically converted to the free basic version. This does not affect data access.

The terms and conditions of contract for the RSC and the RESOL apps are governed by the applicable terms and conditions of use for these services. The right to extraordinary termination with good reason remains unaffected.

When termination takes effect, the data holder is entitled to disable active and continuous data access (e.g. via the REST API or web portal) and discontinue the provision of further connected services.

The user is entitled to continue to use the non-personal raw data and pre-processed product data legally received up to the time of termination of the contract for their own internal purposes. There is no obligation for the user to delete this historical data.

However, the user is obliged to immediately delete or return the software, access data, proprietary analysis tools or confidential documents (business secrets of the data holder) provided and to confirm this in writing at the request of the data holder.

Insofar as data was transferred to a third party at the request of the user, this third party's entitlement to further avail of the data ends with the termination of this agreement. The third party is obliged to immediately cease active data access. The handling of the historical data copies already transmitted to the third party and their possible deletion shall be governed by the separate agreement between the data holder and the third party in accordance with section 4.

Irrespective of any termination of this agreement, the user may at any time demand that a continuous disclosure of data to a third party designated by the user be terminated with effect for the future, without this being otherwise affected by this agreement. In this case, the data holder shall immediately cease transmission to the third party.

10. Liability

Liability of the data holder

The data holder shall be liable without limitation for damage resulting from injury to life, body or health, in the event of intent or gross negligence and in accordance with the Product Liability Act. For minor negligence, the data holder shall only be liable in the event of a breach of an essential contractual obligation (cardinal obligation), the fulfilment of which makes the proper execution of the contract possible in the first place and on whose compliance the contractual partner may regularly rely. In this case, liability is limited to the damage typical for the contract and foreseeable at the time of conclusion of the contract. Further liability of the data holder, in particular for lost profit, production downtimes or indirect consequential damage, is excluded insofar as legally permissible.

Liability of the user

The user is liable for all damages and losses incurred by the data holder as a result of the use of the data provided in breach of contract or law. This applies in particular to damages resulting from a violation of the ban on developing competing products and for damages resulting from the user circumventing technical protective measures (e.g. encryption or access controls), removing them or allowing them to be circumvented by third parties.

Liability in the event of the disclosure of data to third parties

If the user requests the transfer of data to a third party, the user is responsible for the careful selection and authorisation of that third party.

The user indemnifies the data holder from all legitimate third-party claims and damages resulting from the third party named by the user using the data outside the legal requirements of the EU Data Act, unlawfully passing it on or violating agreed protective measures for business secrets, unless the user can prove that they are not responsible for the injury.

11. Order of precedence of legal rights

The above provisions of this agreement (in particular the liability limitations in section 10) only apply if they comply with the mandatory legal provisions of the EU Data Act, the GDPR and the provisions governing contract abuse controls (Art. 13 EU Data Act). These regulations neither exclude nor inadmissibly limit the user's legal claims for data access.

In the event of contradictions between the provisions of this agreement, the provisions of the EU Data Act and the provisions of data protection law, the provisions of the General Data Protection Regulation (GDPR) and the Federal Data Protection Act (BDSG) always take unlimited priority.

The parties acknowledge that the right of the database manufacturer (in accordance with regulation 96/9/EC or § 87a ff. Copyright Act) shall not be used by the data holder to restrict, complicate or deny the legal access and transfer rights of the user under the EU Data Act.

12. Final provisions

Contract changes and presumption of consent

Changes and additions to this agreement must be made in writing (e.g. e-mail). The data holder shall notify the user of amended conditions in writing at least six weeks before their planned entry into force. The user's consent is deemed to have been given if they have not declared their rejection in writing before the proposed date of entry into force of the changes.

In the change notification, the data holder shall draw the user's attention in particular to the right to object, the time limit applicable for this purpose and the legal consequence of silence.

If the user objects to the changes in due time, the contract will be continued under the previous conditions. In this case, the data holder reserves the right to exercise the ordinary termination of the contractual relationship. The user also has the right to terminate the contractual relationship in writing without notice until the changes come into force.

Out-of-court dispute resolution

In the event of any dispute regarding the performance of the obligations arising from this agreement or the EU Data Act (in particular with regard to the adequacy of technical protective measures or remuneration for third parties), both parties shall have the right to appeal to a certified out-of-court dispute resolution body in accordance with Art. 10 of the EU Data Act. Such dispute resolution is voluntary for both parties. The decision of the dispute resolution body shall be binding on the parties only if they have expressly consented to it in advance. The right to appeal to the ordinary courts remains unaffected by this.

Right of appeal

Without prejudice to the above provision, the user shall also have the right at any time, in accordance with Art. 38 of the EU Data Act, to lodge a complaint for a violation of the provisions of the EU Data Act to a competent authority in accordance with Art. 37 of the EU Data Act.

Applicable law and place of jurisdiction

The law of the Federal Republic of Germany shall apply to the exclusion of the UN Convention on Contracts for the International Sale of Goods (CISG), unless mandatory international or European law (in particular the provisions of the EU Data Act and the GDPR) stipulates otherwise. The exclusive place of jurisdiction for all disputes arising from or in connection with this agreement, insofar as the user is a merchant, entrepreneur, a legal entity under public law or otherwise professionally active, is the registered office of the data holder.

Severability clause

Should any provision of this agreement be or become invalid, the validity of the remaining provisions shall remain unaffected.

13. Contact details

If you have any questions regarding data provision, interface setup or the exercising of your rights under the EU Data Act, please contact:

- **E-mail:** datenschutzbeauftragter@resol.de
- **Telephone:** 0049 (0)2324 9648-0

Appendix 1: Data specification

The parties agree that the specific scope, number and designation of the data points provided are not rigidly contractually defined. The readily available data is dynamically generated during the operation of the product. The actual scope of the data depends on the following factors which pertain to the type and configuration:

- The specific device model and its software/firmware version
- The number and type of sensors actually connected by the user (e.g. temperature sensors, actuators, extension modules)
- The activated functions and output signals (e.g. pump speeds, relay assignments) in the system configuration

The detailed description of all potentially available data points, registers, units and technical formats for each product is conclusively obtained from:

- The technical documentation (user instructions / manual) of the respective device model enclosed with the product or available online
- Where available, the manufacturer-specific interface description (e.g. protocol specification, register list or API documentation) in the currently valid version

These documents are made available to the user prior to the conclusion of the contract or during product delivery and are considered an integral part of this data specification.