# DATA PROCESSING AGREEMENT
# PURSUANT TO ARTICLE 28 GDPR

Version 1.0 – as of 12 October 2026

between the controller

The customer within the meaning of the General Terms and Conditions (GTC) of the Processor for whom the respective workspace within the meaning of clause 1.5 of the GTC is set up

– hereinafter referred to as the “Controller” –

and the processor

Kunststoff Information GmbH

– hereinafter referred to as the “Processor” –

– hereinafter jointly referred to as the “Parties” –

# PREAMBLE

This Data Processing Agreement is not concluded as an individual contract but is incorporated via the General Terms and Conditions (GTC) of the Processor. The Processor operates a SaaS platform on which the Controller can set up one or more workspaces within the meaning of clause 1.5 of the GTC. The Agreement is concluded separately for each workspace upon its setup between the Controller (controller) and the Processor (processor). The joining of further users to an existing workspace, invitations, the conclusion or amendment of a subscription and the booking of additional seats do not give rise to any further data processing agreement. No separate signature is required.

The terms and definitions of Regulation (EU) 2016/679 (hereinafter "GDPR"), in particular Article 4 GDPR, shall apply to this Data Processing Agreement.

## 1. SUBJECT MATTER

1.1 The subject matter of this Data Processing Agreement is the determination of the data protection framework for the contractual relationship between the Parties.

1.2 The description of the respective processing, including the subject matter of the processing, the nature and purpose of the processing, the type of personal data and the categories of data subjects, is set out in the Annex under clause 1.

## 2. LOCATION OF PROCESSING

The contractually agreed processing shall take place exclusively in a Member State of the European Union or in another State party to the Agreement on the European Economic Area, unless otherwise provided in the Annex. Before relocating the processing to a third country, the Processor shall inform the Controller in text form (e.g. by e-mail). The Controller may object to the change, stating reasons, in written form or in text form (e.g. by e-mail) within 3 weeks of receipt of the information from the Processor. If no objection is raised within this period, consent to the change shall be deemed to have been given. If a reasoned objection is raised which the Processor cannot remedy by a reasonable adjustment of the processing or in any other reasonable manner, clause 11.6 shall apply accordingly. The processing may only be relocated to a third country if the specific conditions for transfers to a third country under Articles 44 et seq. GDPR are met.

## 3. TERM

3.1 As part of the General Terms and Conditions (GTC) of the Processor, this Agreement takes effect separately for each workspace upon its setup on the Processor's SaaS platform. It shall remain in force for as long as the relevant workspace exists or for as long as the Processor processes personal data of the Controller in connection with the use of that workspace. This

Agreement shall also end upon termination of the workspace. The provisions on the deletion and return of personal data and on confidentiality shall continue to apply after the end of the Agreement.

3.2 The Controller may terminate this Agreement without notice if the Processor commits a serious breach of data protection law or of the provisions of this Agreement. In particular, failure to comply with the obligations agreed in this Agreement and derived from Article 28 GDPR constitutes a serious breach.

## 4. INSTRUCTIONS

4.1 The Processor shall process the personal data only within the scope of the instructions issued by the Controller. This shall not apply where the Processor is required to process the data by Union or Member State law to which the Processor is subject. In such a case, the Processor shall inform the Controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest. The use of the platform's functions by the Controller and its users shall also be deemed an instruction.

4.2 Instructions that amend, revoke or supplement the specifications set out in clause 1 of the Annex shall only be permissible if the Parties enter into a corresponding new agreement in text form.

4.3 Irrespective of the form in which they are issued, both the Processor and the Controller shall document every instruction of the Controller in text form. The instructions shall be retained for the term of this Agreement and for a further three years thereafter.

4.4 The Processor shall inform the Controller without undue delay if, in its opinion, an instruction issued by the Controller infringes statutory provisions. In such a case, the Processor shall be entitled, after giving the Controller timely prior notice, to suspend the execution of the instruction until the Controller has amended or confirmed it. If the Processor can demonstrate that processing in accordance with the Controller's instruction may give rise to liability of the Processor under Article 82 GDPR, the Processor shall be free to suspend further processing to that extent until liability between the Parties has been clarified.

4.5 The Controller shall designate the person or persons authorised to issue instructions. Persons authorised to issue instructions on the part of the Controller are the Workspace Administrator within the meaning of clause 1.5 of the GTC and the users designated by the Controller as admins in the respective workspace. The Controller manages these authorisations on its own responsibility via the platform. The recipient of instructions on the part of the Processor is datenschutz@ki.de. The Processor shall ensure that only authorised employees bound to confidentiality have access to this mailbox. The Controller makes changes to the Workspace Administrator and the admins itself in the application; no separate notification is required.

## 5. ASSISTANCE OBLIGATIONS OF THE PROCESSOR

5.1 Taking into account the nature of the processing, the Processor shall take appropriate technical and organisational measures to assist the Controller in fulfilling its obligation to respond to requests from data subjects under Articles 12 to 22 GDPR.

5.2 Taking into account the nature of the processing and the information available to it, the Processor shall assist the Controller in ensuring compliance with its obligations under Articles 32 to 36 GDPR, specifically with regard to the security of processing, the notification of breaches to the supervisory authority, the communication of a breach to data subjects, the data protection impact assessment and the prior consultation of the competent supervisory authority.

5.3 If a data subject or a data protection supervisory authority contacts the Processor directly in connection with the personal data processed under this Agreement, the Processor shall inform the Controller thereof without undue delay and coordinate the further steps with the Controller.

## 6. AUDIT RIGHTS OF THE CONTROLLER

6.1 At the Controller's request, the Processor shall make available to the Controller the information necessary to demonstrate compliance with the obligations laid down in this Agreement and in Article 28 GDPR. The information shall be limited to information relating to the processing carried out under this Agreement; there shall be no entitlement to the disclosure of trade and business secrets, security-relevant details, personal data of third parties or information of other customers of the Processor.

6.2 The Processor may also demonstrate compliance with its obligations under Article 28 GDPR by submitting suitable documents, in particular current attestations, reports or report extracts from independent bodies (e.g. certified public accountants, internal or external data protection officers, auditors), a suitable certification under an approved certification mechanism within the meaning of Article 42 GDPR, adherence to approved codes of conduct within the meaning of Article 40 GDPR or other suitable documentation of the technical and organisational security concept. Before carrying out an on-site inspection, the Controller shall examine whether the information and evidence provided under clauses 6.1 and 6.2 are sufficient. The right to carry out an on-site inspection under clause 6.3 shall remain unaffected.

6.3 The Controller or a third party commissioned by it and bound to confidentiality shall be entitled to verify compliance with the obligations under this Agreement and under Article 28 GDPR by means of an inspection at the Processor's business premises. The following shall apply to such on-site inspections:

a) the inspection shall be announced in writing or in text form with reasonable notice, as a rule at least four (4) weeks in advance, and its date shall be agreed with the Processor;
b) it shall take place during normal business hours and without avoidable disruption to the Processor's operations;

c) as a rule, it shall take place no more than once per calendar year; this shall be without prejudice to additional inspections where there are specific indications of a breach or on the basis of a binding order of a supervisory authority;
d) the commissioned third party must not be a competitor of the Processor and shall be bound to confidentiality before the inspection;
e) the Controller shall bear its own costs of the inspection; the reasonable effort incurred by the Processor in providing assistance may be remunerated at the Processor's rates applicable from time to time, unless the inspection reveals a breach for which the Processor is responsible;
f) there shall be no access to data, systems and information of other customers of the Processor or to trade and business secrets; where necessary, appropriate protective measures (e.g. anonymisation, accompaniment by the Processor's staff) shall be taken.

The Processor shall enable the inspections permitted under this clause and shall contribute to them to the extent necessary.

## 7. DATA PROTECTION OFFICER OF THE PROCESSOR

The data protection officer of the Processor is named in the Annex to this Agreement under clause 3, insofar as the Processor is required to appoint a data protection officer or has appointed one voluntarily.

## 8. CONFIDENTIALITY

8.1 The Processor confirms that it is familiar with the provisions of the GDPR relevant to processing on behalf of a controller. It shall maintain confidentiality when processing the Controller's personal data. This obligation shall continue to apply after the termination of this contractual relationship.

8.2 The Processor undertakes to familiarise the employees engaged in carrying out the work with the data protection provisions relevant to them. It shall oblige these employees by written agreement to maintain confidentiality for the duration of their activity and also after the end of their employment, unless they are subject to an appropriate statutory obligation of confidentiality. The Processor shall monitor compliance with data protection law within its company.

8.3 The Processor may only provide information to third parties or data subjects with the prior consent of the Controller given in writing or in an electronic format.

## 9. TECHNICAL AND ORGANISATIONAL MEASURES

9.1 The Processor shall implement appropriate technical and organisational measures in such a manner that the processing meets the requirements of the GDPR and ensures the protection

of the rights of the data subject. It shall organise its internal organisation in such a way that it meets the particular requirements of data protection and achieves an appropriate level of protection. In particular, taking into account the state of the art, the Processor shall ensure the appropriate security of processing, in particular the confidentiality (including pseudonymisation and encryption), availability, integrity and resilience of the systems and services used for processing.

9.2 The technical and organisational measures described in clause 5 of the Annex are hereby specified as binding.

9.3 The technical and organisational measures may be adapted to technical developments in the course of the processing relationship. The adapted measures must at least correspond to the level of security of the measures agreed in the Annex under clause 5. Material changes require an agreement in accordance with clause 14.3.

## 10. INFORMATION OBLIGATIONS OF THE PROCESSOR AND PERSONAL DATA BREACHES

10.1 The Processor shall inform the Controller without undue delay of any breaches or suspected breaches of this Agreement or of provisions concerning the protection of personal data.

10.2 The Processor shall assist the Controller in investigating, mitigating and remedying the breaches.

10.3 Should the personal data processed under this Agreement be jeopardised at the Processor by attachment or seizure, by insolvency or restructuring proceedings or by other events or measures of third parties, the Processor shall inform the Controller thereof without undue delay. The Processor shall also inform all bodies concerned in this context without undue delay that control over the data lies with the Controller.

10.4 Where audits are carried out by data protection supervisory authorities, the Processor undertakes to notify the Controller of the result insofar as it concerns the processing of personal data under this Agreement. The Processor shall remedy without undue delay any deficiencies identified in the audit report and inform the Controller thereof.

10.5 This clause 10 shall apply accordingly to incidents in processes carried out by sub-processors.

## 11. SUB-PROCESSORS

11.1 Before engaging or replacing sub-processors, the Processor shall inform the Controller in text form (e.g. by e-mail). The Controller may object to the change, stating reasons, in written form or in text form (e.g. by e-mail) within 3 weeks of receipt of the information from the Processor. If no objection is raised within this period, consent to the change shall be deemed to have been given.

11.2 The Processor shall contractually ensure that the provisions agreed in this Agreement also apply vis-à-vis sub-processors. The Processor's contract with the sub-processor must be concluded in writing or in an electronic format.

11.3 Sub-processors in third countries shall only be engaged if the specific conditions of Articles 44 et seq. GDPR are met.

11.4 The Controller hereby consents to the engagement of the sub-processors listed in the Annex under clause 4.

11.5 The Processor shall ensure that the Controller has the same rights to issue instructions and the same inspection rights vis-à-vis the sub-processor as vis-à-vis the Processor under this Agreement. If a sub-processor fails to fulfil its data protection obligations, the Processor shall be liable to the Controller for the performance of that sub-processor's obligations.

11.6 If a reasoned objection to a new sub-processor is raised pursuant to clause 11.1 which the Processor cannot remedy by a reasonable adjustment of the processing or in any other reasonable manner, each contractual partner shall be entitled to terminate the existing contractual relationship for good cause without observing a notice period, in particular if it cannot reasonably be expected to continue the contractual relationship until the agreed end or until the expiry of a notice period.

11.7 In deviation from clause 11.1, the Processor may replace a sub-processor without prior information if this is necessary to avert an imminent threat to the security or availability of the processing, in particular in the event of a personal data breach at the sub-processor, its insolvency, the discontinuation of its services or the loss of the conditions under Article 28 or Articles 44 et seq. GDPR. The Processor shall inform the Controller thereof in text form without undue delay. The period for an objection under clause 11.1 shall begin upon receipt of this information; clause 11.6 shall apply accordingly. The obligations under clauses 11.2, 11.3 and 11.5 shall remain unaffected.

11.8 Ancillary services which the Processor obtains from third parties and in which no access to the personal data processed on behalf of the Controller in plain text is intended, in particular telecommunications and network services, pure transport and delivery services and the maintenance of hardware without access to data, shall not be deemed sub-processing within the meaning of this clause 11. In these cases, too, the Processor shall make appropriate contractual arrangements and take appropriate control measures to protect the data.

11.9 The sub-processors listed in clause 4 of the Annex in turn engage further sub-processors, which they identify in their own lists provided by them. The authorisation under clause 11.4 extends to these further sub-processors as set out in the current version of these lists from time to time. Clause 11.1 shall not apply to changes to these lists. Through its contracts with its sub-processors, the Processor shall ensure that they impose equivalent data protection obligations on their further sub-processors; clause 13 sentence 2 shall remain unaffected.

## 12. DELETION AND RETURN OF PERSONAL DATA

12.1 The relevant point in time for the end of processing is the termination of the respective workspace, not the termination of a paid subscription. If a paid subscription is terminated while the workspace continues under a free plan, the processing on behalf of the Controller shall continue. After termination of the workspace, the Processor shall be obliged to delete or return all personal data which it has processed on behalf of the Controller in accordance with the following paragraphs. The obligation to delete or return shall not apply if the Processor is legally obliged to continue storing the data under Union or Member State law. If there is a continuing obligation to store the data, the Processor shall restrict the processing of the personal data and use the data only for the purposes for which there is an obligation to store them. The obligations relating to the security of processing shall continue for the period of storage. The Processor shall delete the data without undue delay as soon as the obligation to store them ceases to apply.

12.2 The Controller may request the return of the content created and uploaded by it in text form (e.g. by e-mail) within 30 days of the termination of the workspace. In this case, the Processor shall make the content available in a common, machine-readable format within 14 days of receipt of the request. If the Controller does not request the return within the aforementioned period, deletion shall be deemed to have been chosen.

12.3 The data is removed from production systems as part of ongoing deletion. The Processor creates complete, encrypted snapshots of the application database with rolling retention (2 years), which serve exclusively for recovery after technical failures, faulty migrations and ransomware incidents. Individual records cannot technically be extracted from these snapshots without destroying the integrity of the entire data set. Until final deletion from the backups, the processing of the data concerned is restricted. The data is not actively used or accessed.

12.4 If a backup pursuant to clause 12.3 is restored which contains data already due for deletion pursuant to clause 12 of this Agreement, the data concerned shall be deleted again after completion of the restoration. The process shall be documented.

12.5 Insofar as personal data is still held in backups pursuant to clause 12.3 after the end of the processing relationship, the provisions of this Agreement shall continue to apply to such data – in particular those on confidentiality, technical and organisational measures, instructions and purpose limitation, engagement of sub-processors and inspection and verification rights – until the data has been finally deleted from the backups.

12.6 Deletion shall be carried out in such a way that the data cannot be restored; for data in backups pursuant to clause 12.3, this shall apply at the latest upon expiry of the backup rotation.

12.7 The Processor shall confirm the deletion to the Controller in text form. The Controller shall have the right to verify in an appropriate manner the complete and contractual return or deletion of the data at the Processor. Clause 6 of this Agreement shall apply accordingly.

## 13. LIABILITY

The Processor shall be liable within the scope of the statutory provisions for damage resulting from culpable conduct in breach of data protection provisions or of this Agreement. It shall likewise be liable for culpable conduct of its sub-processors and their sub-processors. The

limitations of liability under clause 11 of the GTC shall also apply to the liability of the Parties to each other arising from or in connection with this Agreement. Liability towards data subjects under Article 82 GDPR shall remain unaffected.

## 14. FINAL PROVISIONS

14.1 The defence of a right of retention within the meaning of § 273 of the German Civil Code (BGB) is excluded with regard to the data processed for the Controller.

14.2 The Annex to this Agreement forms an integral part of it.

14.3 Clause 12.3 of the GTC shall apply to amendments to this Agreement, including its Annex, subject to the proviso that the deemed-consent mechanism shall apply only to non-material amendments. Material amendments, in particular amendments to the specifications in clause 1 of the Annex and material changes to the technical and organisational measures within the meaning of clause 9.3, require the express consent of the Controller in text form. The objection procedures under clause 2 and clause 11.1 shall remain unaffected.

14.4 Should any provision of this Agreement prove to be invalid, this shall not affect the validity of the remaining provisions of the Agreement.

14.5 This Agreement, including its Annex, is provided in German and English. The German version shall be authoritative; in the event of any discrepancies between the language versions, the German version shall prevail.

# ANNEX TO THE DATA PROCESSING AGREEMENT

## 1. SUBJECT MATTER OF THE PROCESSING

### 1.1 Subject matter of the processing:

The subject matter of the processing is the provision and operation of the SaaS platform "pricenxt" for the Controller. This includes in particular the management of memberships, roles and permissions within the workspace as well as storing, displaying and – as specified by the Controller – sharing the content created by its users within the respective workspace. The processing of personal data in connection with user accounts, billing and logging is not the subject matter of this Agreement; in this respect, the Processor is a controller in its own right pursuant to clauses 10.1 and 10.2 of the GTC.

### 1.2 Nature and purpose of the processing:

The Processor processes the personal data provided by the Controller of the users designated by the Controller (for the type of data, see clause 1.3) for the purpose of providing a price information and market intelligence platform for raw material and material prices. This includes in particular the individual compilation and display of price series in a personal dashboard, the creation of notes, the invitation of further users to the workspace and – where used by the Controller – the upload of its own price data by the Controller and – where invoked by the Controller or its users – AI-assisted functions for evaluating workspace content (e.g. reports, summaries, analyses).

### 1.3 Type of data:

| Data category | Specific data processed |
|---|---|
| Professional contact and (work) organisation data | Surname, first name, business e-mail address, form of address |
| Data on professional circumstances | Job title |
| Workspace membership and permission data | Role, invitation status, assigned seat |
| Content created by users | Notes, dashboard configurations and individually compiled price series |
| Own price data uploaded | Own price data optionally uploaded by the Controller |
| AI-assisted evaluation results | Results generated by AI-assisted functions (e.g. reports, summaries, analyses) |
| Personal data of third parties | Personal data of third parties that may be contained in the aforementioned content (e.g. names of business contacts) |

1.4 Categories of data subjects:

| Group of data subjects | Description | Examples |
|---|---|---|
| Employees of the Controller | The Controller's own employees | Employees, freelancers, other persons authorised by the Controller |
| External users | External users invited to the workspace by the Controller | Employees of other companies to whom the Controller has granted access to its workspace |
| Business contacts of the Controller | Business contacts of the Controller, insofar as contained in content | Contact persons at suppliers or customers |

## 2. PERSONS AUTHORISED TO ISSUE INSTRUCTIONS

2.1 Persons authorised to issue instructions on the part of the Controller are:

The Workspace Administrator within the meaning of clause 1.5 of the GTC and the users designated by the Controller as admins in the respective workspace.

2.2 Recipients of instructions at the Processor are:

datenschutz@ki.de

## 3. DATA PROTECTION OFFICER

3.1 The data protection officer of the Processor is:
Proliance GmbH
www.proliance.ai
Data protection officer
Leopoldstr. 21
80802 München, Germany
E-mail: datenschutzbeauftragter@proliance.ai

## 4. SUB-PROCESSORS

The approved sub-processors at the time of conclusion of this Agreement are:

| No. | Sub-processor (name, address, contact) | Data categories processed | Description of the activity | Location of processing |
|---|---|---|---|---|
| 1 | Supabase Pte. Ltd., 65 Chulia Street #38-02/03, OCBC Centre, Singapore | Data categories pursuant to clause 1.3 of the Annex, in | Hosting of the platform's database, file | EU (AWS region Frankfurt). Contractual partner based in |

| | | | | |
|---|---|---|---|---|
| | 049513; contact: legal@supabase.io | particular workspace membership and permission data, content created by users and uploaded files | storage and server-side functions | Singapore; access from outside the EU, in particular for support and administration, cannot be ruled out. Safeguard: EU standard contractual clauses (Module 3) pursuant to the Supabase DPA. |
| 2 | Vercel Inc., 440 N Barranca Ave #4133, Covina, California 91723, USA; contact: ar@vercel.com | Data categories pursuant to clause 1.3 of the Annex, insofar as they are contained in requests to and responses from the application and pass through the hosting infrastructure | Hosting and delivery of the web application app.pricenxt.com | Primarily EU; depending on the location of access, servers outside the EU may also be involved via the global edge network. US company. Safeguard: EU-U.S. Data Privacy Framework and EU standard contractual clauses (Module 3) pursuant to the Vercel DPA. |
| 3 | Lettermint B.V., Willemsvaart 16B, Unit 1.08, 8019 AB Zwolle, the Netherlands (KvK 99337711); contact: legal@lettermint.co | Name and e-mail address of users and invited users as well as the content of e-mails sent from the workspace (e.g. name of the workspace and of the inviting person, notifications about workspace activity); in addition, technical delivery data (delivery status, timestamps) | Sending of e-mails from the workspace (invitations, notifications about workspace activity), including delivery and bounce handling | EU (the Netherlands; backup copies in Germany). No transfer to third countries. |
| 4 | Functional Software, Inc. (Sentry), 45 Fremont Street, 8th Floor, San Francisco, CA 94105, USA | Data categories pursuant to clause 1.3 of the Annex, insofar as | Recording and analysis of application errors | EU (EU data region). US company; access from the USA |

| | | | | |
|---|---|---|---|---|
| | | they are contained in error messages and stack traces (e.g. board or note content) | | cannot be ruled out. Safeguard: EU-U.S. Data Privacy Framework, in the alternative EU standard contractual clauses (Module 3) pursuant to the Sentry DPA. |
| 5 | Acronis International GmbH, Rheinweg 9, 8200 Schaffhausen, Switzerland | Data categories pursuant to clause 1.3 of the Annex as part of encrypted backup copies | Backup and recovery (clause 12.3 of the Agreement) | EU (EU data region). Contractual partner based in Switzerland; access from Switzerland, in particular for support and administration, cannot be ruled out. Transfer on the basis of the European Commission's adequacy decision for Switzerland. |
| 6 | Wasabi Technologies, LLC, 75 Arlington Street, Suite 810, Boston, MA 02116, USA; contact: support@wasabi.com | Data categories pursuant to clause 1.3 of the Annex as part of encrypted backup copies | Object storage for backup copies (clause 12.3 of the Agreement) | EU (EU storage region selected by the Processor). US company; according to the Wasabi DPA, access from outside the selected region is possible. Safeguard: EU standard contractual clauses (Module 3) pursuant to the Wasabi DPA. |
| 7 | Anthropic Ireland, Limited, 6th Floor, South Bank House, Barrow Street, Dublin 4, D04 TR29, Ireland; contact: support@anthropic.com; parent company Anthropic, PBC, San Francisco, USA | Data categories pursuant to clause 1.3 of the Annex, insofar as they are transmitted to the language model when the AI-assisted | Provision of the AI language model (Claude) for the AI-assisted functions under clause 1.2 of the Annex; no use of the data for training AI models | Contractual partner in the EU (Ireland). Processing also in the USA by Anthropic, PBC and further sub-processors of Anthropic. |

| | | | | |
|---|---|---|---|---|
| | | functions are used (e.g. notes, price series, uploaded price data and results generated from them) | | Safeguard for onward transfers: EU standard contractual clauses (Module 3) pursuant to the Anthropic DPA. |

# 5. TECHNICAL AND ORGANISATIONAL MEASURES

## 5.1 Technical and organisational measures in detail

### 5.1.1 Physical access control for premises and facilities in which data is processed

Description: Unauthorised physical access is to be prevented, the term being understood in a spatial sense.

The Processor has taken the following physical access control measures:

- Access control systems for the site, the building and individual rooms/premises in which data processing takes place (e.g. badge readers, magnetic cards, chip cards, keys)
- Door security (security locks, electric door openers, manual/automatic/biometric transponder locking system, etc.)
- Location of the server, e.g. in a room, cabinet, outsourced
- Protection of the server room against access by unauthorised persons
- Number of persons with access to the server room limited to the minimum necessary
- Controlled, documented key issuance, non-duplicable keys, secure storage of additional keys, access cards, etc.
- Servers outsourced outside the company
- Access rules for freelancers/visitors/service providers (e.g. visitors first arrive at a reception and only enter the rest of the building when accompanied)

### 5.1.2 System and data access control

Description: Intrusion by unauthorised persons into the data processing (DP) systems (IT systems) is to be prevented. Likewise, activities in DP systems (IT systems) outside of granted authorisations and unauthorised access to the system from outside are to be prevented.

The Processor has taken the following system and data access control measures (for IT systems):

- Documentation of hardware issued to employees

- Personalised accounts (unique user ID/user assignment), no “account sharing” (use of one account by several persons)
- Individual set-up of access rights (employees’ access rights are restricted to the programs they actually need to use)
- Number of system administrators limited to the minimum necessary
- Login with user ID and password
- Password procedures/password rules (e.g. special characters, minimum length); password policy
- Only one user master record per user/separate user master records
- Differentiated authorisations (profiles, roles, transactions and objects, e.g. restricting access to folders according to the “need-to-know” principle)
- Proper destruction/deletion of data carriers
- Malware protection for the server
- Firewall/antivirus protection for computers/devices
- Incident response management
- Clean desk policy
- Use of password managers to generate and share passwords
- Password encryption (administrators should not be able to view passwords either)
- Authorisation concept
- Two-factor authentication for administrators
- Protection of interfaces against unauthorised intrusion from outside (e.g. Wi-Fi, USB, network sockets)
- Automatic locking of a user after repeated incorrect password entries and measures taken in this case
- Automatic locking (e.g. password or pause function (timeout)/screen lock)
- Organisational arrangements to prevent unauthorised access to personal data at the workplace (e.g. policies)
- Employee training, awareness training
- Evaluations/reports
- VPN technology
- Encryption of data carriers
- Securing of remote maintenance access, servers and end devices, external interfaces (e.g. USB)

### 5.1.3 Input control

Description: The traceability and documentation of data management and maintenance must be ensured. Measures for subsequently verifying whether and by whom data has been entered, modified or removed (deleted).

The Processor has taken the following input control measures:

- Logging of logins and logouts
- Logging of the activities of the IT system itself and of IT administrator activities
- Logging of user activities
- Documentation of maintenance, remote maintenance or repair work carried out on the IT system
- Ensuring the integrity of new programs and updates, e.g. through a process ensuring that employees cannot download or install programs themselves
- Malware check for data carriers received and to be delivered
- Complete backup of the systems concerned before major maintenance/remote maintenance or repair work

### 5.1.4 Processing control

Description: Processing in accordance with instructions must be ensured. Processing by third parties (cf. Article 28 GDPR) is permitted in accordance with the instructions of the Controller/data exporter. Measures (technical and organisational) to delimit the responsibilities between the Controller/data exporter and the Processor/data importer.

The Processor has taken the following processing control measures:

- Criteria for the careful selection of sub-processors
- Clear contract design, written specification of instructions
- Measures ensuring that personal data processed on behalf of the Controller is processed in accordance with the Controller's instructions, e.g. written instructions, documentation of instructions, offer and order confirmation, ensuring that the Processor's employees are bound to confidentiality under data protection law, contractually defined responsibilities (persons authorised to issue instructions and recipients of instructions), regular checks within the company
- Data processing agreements
- Register of all data processing agreements
- Concept for the deletion of data after the end of the contractual relationship

Information on outsourced/externally hosted servers:

- Hosting providers:
  Vercel and Supabase (in each case virtual servers in their cloud infrastructure).

- Server location and transfers to third countries:
  Supabase: the project region is the EU (AWS region Frankfurt); as the contractual partner is based in Singapore, access from outside the EU (in particular support and administration) cannot be ruled out. Such access is safeguarded by the EU standard contractual clauses (Module 3) contained in the Supabase DPA. Vercel is a US company with a global edge network; each request is answered by the geographically nearest server, so that, depending on the user's location of access, servers outside the EU may also be involved. Insofar as this results in transfers to third countries, the requirements of Articles 44 et seq. GDPR are safeguarded by the EU-U.S. Data Privacy Framework and the EU standard contractual clauses (Module 3) contained in the Vercel DPA.

- Security evidence of the hosting providers:
  Data Processing Agreements (DPAs) are in place with both providers. SOC 2 Type II audit reports are available for Vercel and Supabase.

- Securing of the connection to the servers:
  All connections are made exclusively in encrypted form via TLS (HTTPS); access to the hosting providers' APIs is via individual API keys/credentials issued according to the principle of least privilege.

### 5.1.5 Separate processing of data/separation control

Description: The separate processing of data collected for different purposes must be ensured. Measures for the separate processing of the data of different controllers must be ensured.

The Processor has taken the following separation control measures:

- Separation of data relating to different customers/controllers
- Separation of data processed for different purposes
- Use of different, customer-specific or multi-tenant systems
- Separation of functions (production/test)
- Compliance with different deletion periods is ensured

### 5.1.6 Transfer control

Description: Aspects of the disclosure of personal data are to be regulated (electronic transmission, data transport, transfer control, etc.) in order to prevent loss, alteration or unauthorised publication. Measures for transport, transmission, transfer or storage on data carriers (manual or electronic) and for subsequent verification are to be taken.

The Processor has taken the following transfer control measures:

- Wi-Fi access secured
- Protection of data during electronic transmission
- E-mail encryption (SSL, TLS, etc.)
- Transport security (e.g. courier, locked containers)
- Secure destruction of data carriers no longer required
- Proper disposal of paper files no longer required
- Tunnel connection (VPN = virtual private network)
- Encrypted platforms for the transfer of data

### 5.1.7 Availability and resilience (Article 32(1)(b) GDPR)

Description: The data must be protected against accidental destruction and loss. Measures for data backup (physical/logical).

The Processor has taken the following availability and resilience control measures:

- Regular data backups/backup procedures, resilience of IT systems
- Measures to secure the (own) server room and the IT infrastructure
- Emergency plan for IT emergencies (disaster recovery plan) and for personal data breaches
- Clear reporting channels for IT emergencies and personal data breaches
- Antivirus, firewall, anti-spyware, spam filter, IDS or IPS systems
- Fire alarm system

### 5.1.8 Organisational control

Description: How is the smooth organisation of data protection and data security ensured within the company?

The Processor has taken the following organisational control measures

- Written commitment of all employees to confidentiality under data protection law
- Procedures for risk assessment and risk management established and documented
- Policy on the use of the company internet access and the company e-mail account
- Regular awareness-raising/training of employees, policies/manuals for employees
- Organisation of the implementation of data protection (e.g. appointment of a data protection officer; internal employees supporting the data protection officer)

- Preparation of a data protection concept
- IT security concept in place
- Policy/work instruction on handling personal data when working from home/mobile working

### 5.1.9 Privacy by default and privacy by design

Description:
Privacy by default means “data protection by default”. This means that even the factory settings should be designed to be privacy-friendly. This is intended above all to protect users.
Privacy by design means “data protection by design”. This means that attention should be paid to privacy-friendly design already when developing or purchasing software.

The Processor has taken the following measures:

Privacy by default:
- Transparent settings and options for the user to choose the settings.
- Default settings under which the software only collects the data that is strictly necessary.

Privacy by design:
- When developing or purchasing software, care is taken to ensure that the software requests/requires as little data as possible for processing

### 5.1.10 Effectiveness control

Description: All actions leading to evidence that the measures implemented are effective.

The Processor has taken the following effectiveness control measures:

- Regular checks of the effectiveness of the technical and organisational measures implemented
- Regular checks of the functionality of the antivirus software and the firewall