Recyda Data Processing Agreement

Recyda GmbH, Kaiser-Joseph-Straße 254, 79098 Freiburg im Breisgau, Germany ("Processor" in the following section) processes personal data on behalf of the customer ("Controller" in the following section). This contract contains the written order within the meaning of Article 28 of the General Data Protection Regulation ("GDPR") and regulates the rights and obligations of the Parties in connection with the processing of personal data on behalf of Controller.

1. Subject matter and duration of the contract

1.1 Personal data are processed within the provision of the following services:

Processor provides Controller with a software and database on international packaging recyclability ("Services"). Processor manages the hosting and operations of the Services.

1.2 The duration of this contract corresponds to the duration of the Services.

1.3 Controller may terminate this contract at any time without notice if Processor is in serious breach of the provisions of this contract, if Processor is unable or unwilling to carry out instructions from Controller or if Processor refuses to comply with contractual or statutory control measures of Controller.

2. Specification of processing

2.1 The processing of personal data shall be carried out exclusively within a member state of the European Union (EU) or within a member state of the European Economic Area (EEA). Each and every transfer of personal data to a state which is not a member state of either the EU or the EEA requires the prior approval of Controller and shall only occur if the specific conditions of Article 44 et seq. GDPR are met.

2.2 The following data types/categories are subject to the processing of personal data:

- personal master data, such as name, surname, company name

- communication data, such as email address, phone number

- location data, such as country, city

- contract master data, such as subscription data

- logging data

2.3 The following data subjects are subject to the processing of personal data:

- users of the Services

3. Technical and organisational measures

3.1 Processor shall establish security in accordance with Articles 28(3)c, 32 GDPR. The measures to be taken are measures of data security and measures that guarantee a protection level appropriate to the risk concerning confidentiality, integrity, availability and resilience of the systems. The state of the art, implementation costs, the nature, scope and purposes of processing as well as the probability of occurrence and the severity of the risk to the rights and freedoms of natural persons within the meaning of Article 32(1) GDPR must be taken into account. Processor's technical and organisational measures are subject to **Appendix 1**.

3.2 The technical and organisational measures are subject to technical progress and further development. In this respect, it is permissible for Processor to implement alternative adequate measures that do not reduce the overall security level. Substantial changes must be documented.

4. Quality assurance and other duties of Processor

4.1 Processor shall comply with the statutory requirements referred to in Articles 28 to 33 GDPR; accordingly, Processor ensures, in particular, compliance with the following requirements:

- If required by applicable law, Processor shall appoint a data protection officer and submit his/her contact detail (publication on Processor's website is sufficient).

- Processor entrusts only such employees with the data processing outlined in this contract who have been bound to confidentiality. Processor and any person acting under its authority who has access to personal data, shall not process that

data unless on instructions from Controller, which includes the powers granted in this contract, unless required to do so by law.

- Processor shall cooperate in an appropriate manner in the preparation of the record of processing activities (Article 30(1) GDPR) by the Controller by providing relevant information. In addition to his own record of processing activities, Processor must maintain its own list in accordance with the requirements of Article 30(2) GDPR for all categories of processing activities carried out on behalf of Controller.

- Controller and Processor shall cooperate, on request, with the supervisory authority in performance of its tasks.

- Controller shall be informed immediately of any inspections and measures conducted by a supervisory authority, as far as they relate to this contract.

4.2 Processor may not on its own authority rectify, erase or restrict the processing of personal data that is being processed on behalf of Controller, but only on documented instructions of Controller. In case a data subject contacts Processor directly concerning rectification, erasure, or restriction of processing, Processor will immediately forward the request to Controller.

5. Subprocessing

5.1 Subprocessing for the purpose of executing this contract is to be understood as meaning services which relate directly to the provision of the main service. This does not include ancillary services, such as telecommunication services, postal / transport services, maintenance and user support services or the disposal of data carriers, as well as other measures to ensure the confidentiality, availability, integrity and resilience of the hardware and software of data processing equipment. Nonetheless, Processor shall be obliged to make appropriate and legally binding contractual arrangements and take appropriate inspection measures to ensure data protection and data security of Controller's data, even in the case of such ancillary services.

5.2 Processor may commission subprocessors. Controller agrees to the following subprocessors:

Subprocessor	Address	Service
Microsoft	Microsoft Deutschland GmbH Walter-Gropius-Strasse 5 80807 München Germany	Hosting, Data Center Operation
Amazon Web Services	Amazon Web Services EMEA SARL 38 Avenue John F. Kennedy, L-1855 Luxembourg	Hosting, Data Center Operation
Google Cloud	Google Cloud EMEA Limited 70 SIR JOHN ROGERSON'S QUAY, 662881, Ireland	User Authentication, AI services
CloudFlare	Cloudflare, Inc. 101 Townsend St. San Francisco, CA 94107 USA	DDoS protection, Web Application Firewall, Domain Name System Management
Hubspot	Hubspot Germany GmbH Am Postbahnhof 17 10243 Berlin	Customer relationship management
ArangoDB	ArangoDB GmbH Hohenstaufenring 43-45 50674 Cologne Germany	Hosting, Database Operation
Custify	Custify S.R.L Zagazului Street, No. 4E, Entrance A, First Floor, ap. 1A, District 1 Bucharest Romania	Customer relationship management
AI subprocessors (only if using AI services):		
OpenAI	3180 18th St., San Francisco, CA 94110. UNITED STATES	AI services
Anthropic	Anthropic Ireland, Limited 6th Floor South Bank House, Barrow Street, Dublin 4, Dublin, Ireland	AI services
Langfuse	Langfuse GmbH Gethsemanestr. 4, 10437 Berlin, Germany	AI services

5.3 Processor shall inform Controller of any intended change with regard to subprocessors or the replacement of existing subprocessors Controller in writing or in text form with appropriate advance notice, which will enable the the possibility to object to such changes for legitimate reasons. If the Processor is unable to perform the contract without the indicated change, the Processor may terminate the agreement for cause following an objection by the Controller.

5.4 Processor shall carefully select subprocessors and ensure compliance with the provisions set out in this contract. Further outsourcing by subprocessors requires that the terms of this contract are complied with.

6. Supervisory powers of Controller

6.1 Controller has the right, after consultation with Processor, to carry out inspections or to have them carried out by a competent third party.

6.2 Processor shall ensure that Controller is able to verify compliance with the obligations of Processor in accordance with Article 28 GDPR.

7. Communication in the case of infringements by Processor

7.1 Processor shall assist Controller in complying with the obligations concerning the security of personal data, reporting requirements for data breaches, data protection impact assessments and prior consultations, referred to in Articles 32 to 36 GDPR. These include:

- Ensuring an appropriate level of protection through technical and organizational Measures that take into account the circumstances and purposes of the processing as well as the projected probability and severity of a possible infringement of the law as a result of security vulnerabilities and that enable an immediate detection of relevant infringement events;
- the obligation to report a personal data breach immediately to Controller;
- the duty to assist Controller with regard to Controller's obligation to provide information to data subjects and to immediately provide Controller with all relevant information in this regard;

- supporting Controller, if necessary, with its data protection impact assessment;
- supporting Controller, if necessary, with regard to prior consultation of the supervisory authority.

8. Authority of Controller to issue instructions

8.1 Controller reserves the right to issue comprehensive instructions on the type, scope and procedure of data processing, which can be specified by means of individual instructions. Changes to the subject of processing and procedural changes shall be made in accordance with the instructions of Controller and shall be documented. If changes to the processing are implemented, Processor must be informed immediately.

8.2 Controller shall immediately confirm oral instructions (at the minimum in text form).

8.3 Processor shall inform Controller immediately if an instruction is considered to violate any applicable data protection regulations. Processor shall then be entitled to suspend the execution of the relevant instructions until Controller confirms or changes them.

9. Deletion, return and further use of personal data

9.1 Copies or duplicates of the data shall never be created without the knowledge of Controller, with the exception of back-up copies as far as they are necessary to ensure orderly data processing, as well as data required to meet regulatory requirements to retain data.

9.2 After conclusion of the data processing governed by this contract, or earlier upon request by Controller, at the latest upon termination of the agreement, Processor shall hand over to Controller or – subject to prior consent – destroy all documents, processing and utilization results, and data sets related to the contract that have come into its possession, in a data-protection compliant manner. The same applies to any and all connected test, waste, redundant and discarded material. The log of the destruction or deletion shall be provided on request.

9.3 Documentation which is used to demonstrate orderly data processing shall be stored beyond the contract duration by Processor in accordance with the respective retention periods.

Appendix 1: technical and organisational measures

1. Electronic Access Control

Measures and protocols to prevent unauthorised persons to use data processing systems

- ✓ assignment of user rights
- ✓ creation of user profiles
- ✓ password assignment
- ✓ assignment of user profiles within IT-system
- ✓ authentification by username/password
- ✓ encryption of data carrier within laptops/notebooks
- ✓ use of software firewall

2. Internal Access Control

Measures and protocols to ensure that the access to data processing system of any person granted user rights under the authority of the Processor is limited to the granted rights and that personal data cannot be read, copied, changed or deleted within the system when processed, used or after storage.

- ✓ number of administrators limited to the minimum
- ✓ management of rights by system administrator
- ✓ recording of access to systems, esp. when entering, changing or deleting data
- ✓ password policy including length and change of password

3. Separation rule

Measures and protocols to ensure that data which have been collected for different purposes can be processed separately

- ✓ logical client separation (by software)
- ✓ separation of productive systems from test-systems

4. Data Entry Control

Measures and protocols to ensure subsequent verification and determination whether and by whom data is entered, changed or deleted in a data processing system

- ✓ recording of entry, change and deletion of data
- ✓ control by logfile-system
- ✓ assignment of rights to enter, change or delete data based on authorization concept

5. Order Control

Measures and protocols to ensure personal data processed in order and on behalf of contracting party will only be processed for the performance of the contract and according to the instructions of contracting party

✓ written instructions by contractor (e.g. through Data Processing Agreement)

6. Availability Control

Measures and protocols to prevent personal data of accidental destruction or loss.

✓ regular backup copies

7. Procedures for regular testing, assessment and evaluation (Article 32(1)d GDPR; Article 25(1) GDPR)

The adopted measures and protocols shall undergo regular assessment. The measures shall undergo technology upgrading and are to be kept up to date. Within the company, the control- and evaluation concept will be implemented as follows.

✓ regular monitoring of technical components of the backup- and recovery concept

✓ regular installation of patches and software updates