Data Processing Agreement

Provisions on data protection and data security for commissioned data processing

concluded by and between

CONTROLLER

Name: _____

Address: _____

_____

Contact Person: _____

Email: _____

– Controller – (hereinafter referred to as "the Controller", which term shall include "Business" as defined under the California Consumer Privacy Act where applicable)

and

saas.group LLC (operating the Juicer.io platform), 304 S. Jones Blvd #1205 Las Vegas, Nevada, 89107 USA

– Processor – (hereinafter referred to as "the Processor", which term shall include "Service Provider" as defined under the California Consumer Privacy Act where applicable)

(Both jointly hereinafter referred to as "Parties")

Preamble

In order to specify the rights and obligations arising from the contractual data processing relationship in accordance with the statutory obligation under Art. 28 of the EU General Data Protection Regulation (EU GDPR), the UK General Data Protection Regulation (UK GDPR), and to ensure compliance with the California Consumer Privacy Act (CCPA) and other applicable data protection laws, the contracting Parties conclude the following agreement.

Definitions

For the purposes of this Agreement, the following terms shall have the meanings set forth below:

"Data Protection Legislation" means any applicable legislative or regulatory regime enacted by a recognized government, or governmental or administrative entity with the purpose of protecting the privacy rights of natural persons, including (without limitation): - The General Data Protection Regulation (EU) 2016/679 ("**EU GDPR**"); - The EU GDPR as saved into United Kingdom law by virtue of Section 3 of the United Kingdom's European Union (Withdrawal) Act 2018, and the United Kingdom's Data Protection Act 2018 ("**UK GDPR**"); - The California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act of 2020 ("**CCPA**"), Cal. Civ. Code § 1798.100 et seq.

"Controller", **"Processor"**, **"Data Subject"**, **"Personal Data"**, **"Personal Data Breach"**, and **"Processing"** have the meanings given to them in the Data Protection Legislation. For the purposes of this Agreement: (i) references to "Processor" shall be interpreted to include equivalent terms under applicable Data Protection Legislation, including "Service Provider" as defined under the CCPA; and (ii) the use of the term "Process" shall be interpreted in accordance with the definition of "Processing" under the relevant Data Protection Legislation.

"Standard Contractual Clauses" means: (i) where the EU GDPR applies, the Processor's EU Standard Contractual Clauses (Module Two: Controller to Processor) pursuant to European Commission Implementing Decision 2021/914; and/or (ii) where the UK GDPR applies, the Processor's International Data Transfer Addendum to the EU Commission Standard Contractual Clauses (UK ICO Version B1.0).

---

1. Subject matter, nature and purpose of processing

(1) Juicer provides social media aggregation and feed curation software that enables businesses to embed, curate, and aggregate social media content from multiple platforms into unified social media feeds displayed on their websites.

(2) Furthermore, the subject matter of the processing arises from the Terms of Use available at https://www.juicer.io/terms (hereinafter referred to as "Main Agreement"), to which this refers to.

An additional processing of personal data of the Controller by the Processor is not intended.

---

2. Categories of personal data and data subjects

(1) **Categories of personal data processed:**

- Identification data: names, email addresses
- Technical data: IP addresses (processed as necessary for TCP/IP communication and delivery of service content to the requesting client; not persistently stored)

- Social media data: social media handles, publicly accessible social media content
- Transaction data: customer purchase information (processed with limited access via third-party payment processor; complete payment credentials remain inaccessible to the Processor)
- Communication and contact data as specified in the Main Agreement
- Additional categories as described in the Processor's Privacy Policy available at https://www.juicer.io/privacy

(2) **Categories of data subjects whose personal data is processed:**

- The Controller's organization and its authorized users (including officers, employees, agents, and contractors)
- End users accessing the Controller's website
- Third-party individuals whose publicly available social media content is aggregated through the Processor's platform

---

3. Duration of the commission

The duration of this commission ("Term") corresponds to the duration of the Main Agreement and ends upon deletion of Controller's data as stipulated by the Agreement.

---

4. Responsibility and authority to issue instructions

(1) The Controller is responsible for compliance with data protection regulations, in particular for the lawfulness of data transfer to the Processor and for the lawfulness of data processing (Art. 4 no. 7 EU GDPR / UK GDPR). The Processor shall not use the data for any other purpose and in particular shall not be entitled to pass them on to third parties. Copies and duplicates will not be made without the Controller's knowledge. Exceptions shall apply only to the extent specified in paragraph 2 of this clause.

(2) The Processor processes personal data only on documented instruction from the Controller, unless otherwise required under Union law, the law of the Member State to which the Processor is subject, or applicable US state or federal law. Personal information will not be retained, used, or disclosed for any purpose other than as necessary for providing services as specified in the Main Agreement or as otherwise required by law. In the event of any contrary obligation, the Processor shall inform the Controller of the corresponding legal requirements before processing.

(3) If the Processor is of the opinion that an instruction infringes data protection regulations, the Processor shall inform the Controller without delay in accordance with Article 28 para. 3 sentence 3 EU GDPR / UK GDPR. The Processor shall be

entitled to suspend the execution of the instruction until such instruction has been confirmed or changed.

5. Confidentiality

The Processor shall only employ persons for the execution of the work who have committed themselves to confidentiality in accordance with Art. 28 para. 3 sentence 2 lit. b EU GDPR / UK GDPR and who have previously been acquainted with the data protection provisions relevant to them. The Processor and any person under the Processor's control who has access to personal data may process such data exclusively in accordance with the instructions of the Controller, including the powers conferred in this Agreement, unless they are under a statutory obligation to process the data.

6. Data Security

(1) The Processor shall take appropriate technical and organizational measures for the appropriate protection of personal data, in accordance with Art. 28 para. 3 lit. c EU GDPR / UK GDPR in conjunction with Art. 32 para. 1 EU GDPR / UK GDPR, in order to guarantee the security of the processing by the Processor. For this purpose, the Processor shall:

- ensure the confidentiality, integrity, availability and resilience of systems and services in connection with processing in the long term,
- ensure the ability to quickly restore the availability of and access to personal data in the event of a physical or technical incident; and
- maintain a procedure for the regular review, assessment and evaluation of the effectiveness of technical and organizational measures to ensure the safety of processing.

The state of the art, the costs of implementation and the nature, scope and purpose of processing, as well as the risk of varying likelihood and severity of the risk for the rights and freedoms of natural persons within the meaning of Art. 32 para. 1 EU GDPR / UK GDPR must be taken into account.

(2) The contracting Parties agree on the data security measures laid down in **Annex 1 "Technical and organizational measures"** to this Agreement.

(3) The technical and organizational measures are subject to technical progress and further development. In this respect, the Processor is permitted to implement alternative adequate measures. The safety level may not fall below the specified measures. Significant changes must be documented and communicated to the Controller in writing.

7. Engagement of other processors (subcontractors)

(1) For the purposes of this provision, subcontractors shall be processors commissioned by the Processor whose services relate directly to the provision of the main service. This does not include ancillary services used by the Processor, for example, telecommunication services, postal/transport services and cleaning. However, the Processor is obliged to take appropriate and legally compliant contractual agreements and control measures to guarantee data protection and data security of the Controller's data, even in the case of outsourced ancillary services.

(2) The outsourcing to subcontractors or the change of the existing subcontractor is permitted, as far as:

- the Processor notifies the Controller in advance with a reasonable period of time (at least 30 days) in writing or in text form of such outsourcing to subcontractors, and
- the Controller does not raise an objection against the planned outsourcing in writing or in text form until the date of handover of the data to the Processor.

(3) A contractual agreement is to be concluded with the subcontractor in accordance with Art. 28 para. 3 and 4 EU GDPR / UK GDPR, which meets the requirements for confidentiality, data protection and data security of this Agreement. The Controller shall be entitled to inspect the Processor's contracts with subcontractors and to demand that the Processor send a copy of these contracts.

(4) The transfer of the Controller's personal data to the subcontractor and the subcontractor's first action shall only be permitted if all the prerequisites for subcontracting are met. The subcontractors approved by the Controller at the time of conclusion of the contract are listed in **Annex 2** to this contract.

(5) If the subcontractor provides the agreed service outside the EU/EEA or UK, the Processor shall ensure the admissibility with regard to data protection law by means of appropriate measures.

(6) Further outsourcing by the subcontractor requires the express consent of the Controller (at least in text form). All contractual provisions in the contract chain must also be imposed on the other subcontractors.

8. Cross-border data transfers

(1) Where the Processing of Personal Data protected by EU GDPR involves transfers outside the EEA, or where the Processing of Personal Data protected by UK GDPR involves transfers outside the UK, to territories without an

adequacy decision, the Processor shall ensure compliance with applicable Data Protection Legislation.

(2) The Processor offers Standard Contractual Clauses as separate agreements to facilitate lawful cross-border transfers:

- **EU Standard Contractual Clauses (EU SCCs):** For transfers subject to EU GDPR, the Processor's EU SCCs (Module 2: Controller to Processor) pursuant to European Commission Implementing Decision 2021/914 are available upon request or at the Processor's website.
- **UK Addendum:** For transfers subject to UK GDPR, the Processor's International Data Transfer Addendum to the EU Commission Standard Contractual Clauses (UK ICO Version B1.0) is available upon request or at the Processor's website.

(3) Controllers requiring such transfer safeguards may execute the appropriate Standard Contractual Clauses agreement(s) by contacting privacy@juicer.io.

(4) For transfers subject to CCPA, the Processor shall comply with applicable cross-border transfer requirements as specified in California law.

---

9. Support in protecting the rights of data subjects

(1) The Processor is obliged to support the Controller with appropriate technical and organizational measures to protect the rights of the data subjects as specified in Art. 12 to 22 EU GDPR / UK GDPR (Art. 28 para. 3 sentence 2 lit. e EU GDPR / UK GDPR). In particular, the Processor shall support the Controller in fulfilling the claims of data subjects for deletion of their personal data in accordance with Article 17 EU GDPR / UK GDPR and in responding to requests under the CCPA including, but not limited to, rights to access, delete, and opt-out of the sale of personal information.

(2) If data subjects are able to exercise the right to data portability against the Controller, the Processor shall ensure that they can receive the data, which they have provided to the Controller, in a structured, commonly used and machine-readable format.

(3) The Processor may only correct, delete or restrict the processing of personal data in accordance with documented instructions from the Controller. The Processor may only provide information to third parties or the persons concerned after prior written consent by the Controller.

(4) If a data subject contacts the Processor directly in order to assert his rights in accordance with Articles 12 to 22 of the EU GDPR / UK GDPR or under the CCPA, the Processor will forward the request to the Controller promptly.

---

10. Personal Data Breach notification

(1) If the Processor becomes aware of a Personal Data Breach, the Processor shall notify the Controller without undue delay after having become aware of the breach.

(2) Such notification shall contain, to the extent possible:

- A description of the nature of the Personal Data Breach including the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
- The name and contact details of the Processor's data protection contact point where more information can be obtained;
- A description of the likely consequences of the Personal Data Breach;
- A description of the measures taken or proposed to be taken by the Processor to address the Personal Data Breach, including measures to mitigate its possible adverse effects.

(3) Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(4) The Processor shall cooperate with and assist the Controller to enable the Controller to comply with its obligations under the Data Protection Legislation, including breach notification requirements under EU GDPR, UK GDPR, CCPA and other applicable US state laws.

---

11. Data Retention and Deletion

(1) Personal data will be deleted or returned to the Controller as described in Juicer's data retention policy:

- Contact details (name, email, address, etc.) are retained for 2 years after account deletion to enable customer identification and support as described in the Privacy Policy
- Social media posts and handles are deleted within 62 days after account deletion to enable restoration in case of accidental account cancellation
- Unless otherwise required by applicable law or as specified in the Main Agreement

(2) The Processor shall document and certify to the Controller that all data has been deleted or returned in accordance with this Agreement upon the Controller's request.

---

12. CCPA-Specific Obligations

(1) **No Sale of Personal Information.** The Processor certifies that it does not and will not sell personal information as that term is defined in the California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act of 2020 (collectively, "CCPA"), Cal. Civ. Code § 1798.100 et seq.

(2) **Service Provider Limitations.** The Processor shall not retain, use, or disclose personal information provided by or on behalf of the Controller except as necessary for the specific purpose of performing the services specified in the Main Agreement, or as otherwise permitted by the CCPA. The Processor shall not retain, use, or disclose such personal information for a commercial purpose other than providing the services specified in the Main Agreement, or as otherwise permitted by the CCPA, including by retaining, using, or disclosing personal information for a commercial purpose other than providing the services specified in the Main Agreement.

(3) **Right to Delete.** The Processor shall delete or enable the Controller to delete personal information about California consumers upon the Controller's request, unless an exception applies under CCPA § 1798.105(d).

(4) **Certification of Understanding.** The Processor certifies that it understands the restrictions set forth in this Section 12 and will comply with them.

---

13. Support with documentation and reporting obligations

(1) If, according to Art. 37 EU GDPR / UK GDPR the Processor is legally obliged to appoint a data protection officer, the Processor shall inform the Controller of the data protection officer's contact details for the purpose of direct contact. A change of the data protection officer must be reported to the Controller immediately.

(2) As designated contact person for data protection matters, Petr Chalupa, CTO of Juicer, has been appointed.

- Contact email: privacy@juicer.io
- Address: 304 S. Jones Blvd #1205, Las Vegas, Nevada, 89107, USA

(3) The Processor shall support the Controller with all information at his disposal in fulfilling the information obligations in relation to the competent supervisory authority in accordance with Art. 33 EU GDPR / UK GDPR and, if applicable, in relation to the data subjects affected by the violation of the protection of personal data in accordance with Art. 34 EU GDPR / UK GDPR, as well as any notification requirements under the CCPA and other applicable US laws.

(4) The Processor shall support the Controller with all information at his disposal in the data protection impact assessment pursuant to Art. 35 EU GDPR / UK GDPR and, if necessary, in a prior consultation with the competent supervisory authority pursuant to Art. 36 EU GDPR / UK GDPR.

(5) The Processor shall inform the Controller without delay of any checks and measures taken by the supervisory authority insofar as they relate to this Agreement.

14. Termination of the commission

(1) At the choice of the Controller, the Processor deletes or returns all the personal data to the Controller after the end of the provision of services relating to processing, and deletes existing copies unless Union or Member State law or applicable US law requires storage of the personal data.

(2) The Processor shall, without explicit request, prove to the Controller in text form with date indication that he has returned all data carriers and other documents to the Controller or that he has destroyed or deleted them in accordance with data protection regulations and has therefore not retained any of the Controller's data.

(3) The Processor shall keep any and all documentation which serves as evidence of the orderly and lawful data processing for the Controller beyond the end of the contract. The Processor can return them to the Controller at the end of the contract for his discharge.

15. Control rights of the Controller

(1) The Controller is entitled to regularly check the technical and organizational measures as well as compliance with this Agreement and data protection regulations before and during the provision of services relating to processing. For this purpose, the Controller or an authorized auditor may inspect the data processing equipment and the data processing systems of the Processor.

(2) For this purpose, the Processor shall be obliged to grant the Controller, during normal business hours and with reasonable advance notice (at least 30 days), access to the premises where the Controller's data are physically or electronically processed. The Controller coordinates the inspections with the Processor in such a way that the operating procedures of the Processor are affected as little as possible.

(3) The Processor shall provide the Controller with all necessary information to prove the technical and organizational measures as well as compliance with this Agreement and data protection regulations. This information especially includes

current attestations, reports or report extracts from independent bodies (e.g. financial auditors, external experts, IT security or data protection auditors) and suitable certification (e.g. according to the Basic Protection of the BSI – German Federal Office for Information Security). The Processor provides immediately the Controller with specific information on a case-by-case basis.

16. Warranties

(1) The Processor warrants and represents that:

- (a) It and anyone operating on its behalf will Process the Personal Data in compliance with the Data Protection Legislation;
- (b) Considering the current technology environment and the Processing involved, it will maintain appropriate technical and organizational measures to ensure an adequate level of security as described in Section 6;
- (c) It shall ensure that any persons involved in the Processing of the Personal Data on its behalf, including its employees, agents, contractors and subcontractors, are adequately trained and aware of their responsibilities regarding the protection of the Personal Data.

17. Liability

(1) According to Art. 82 para. 1 and 4 EU GDPR / UK GDPR, the Controller and the Processor are liable in their external relationship for the material and immaterial damage suffered by a person as a result of an infringement of the EU GDPR, UK GDPR or applicable data protection laws including the CCPA. If both the Controller and the Processor are responsible for such damage, the Parties are internally liable for this damage in proportion to their share of the responsibility. If, in such a case, a person claims damages from one party in whole or in part, the other party can demand indemnification or indemnity from the other party corresponding to its part of responsibility for the damage.

18. Notice

(1) All notices required or permitted under this Agreement shall be sent via email to the email address provided by the receiving Party in the signature section of this Agreement or as otherwise designated by such Party in writing.

(2) Notices shall be deemed given upon confirmation of receipt of the email transmission.

(3) Either Party may change its designated email address for notices by providing written notice to the other Party.

19. Final provisions

(1) Data carriers and data records provided to the Processor remain the property of the Controller.

(2) If individual or several clauses of this Agreement should be ineffective, the effectiveness of the remaining agreement is not affected. In the event that individual or several provisions of the contract are invalid, the Parties shall immediately replace the invalid provision with a provision which most closely resembles the invalid provision in terms of commercial interests and data protection.

(3) In the event of a contradiction between the Main Agreement and this Agreement, this Agreement shall take precedence in so far as the contradiction concerns the processing of personal data.

(4) All services provided by the Processor in connection with the fulfillment of his obligations under this Agreement shall be settled with the remuneration from the Main Agreement.

(5) **Governing law and venue.** This Data Processing Agreement is subject to German law.

(6) The following Annexes form an integral part of this Agreement:

- Annex 1 “Technical and organizational measures”
- Annex 2 “Approved subcontractors”

Signatures

FOR THE CONTROLLER:

Place: _____

Date: _____

Name (Print): _____

Title: _____

Signature: _____

FOR THE PROCESSOR (saas.group LLC):

Place: Las Vegas, Nevada, USA
Date: Oct 20, 2025
Name (Print): Ulrich Essmann
Title: President, saas.group LLC
Signature: 

Annex 1

Technical and organizational measures

Clause 6 of the Commissioned Data Processing Agreement refers to this annex for the specification of the technical and organizational measures.

1. Confidentiality (Art. 32 para. 1 lit. b GDPR)

1.1 Access control to premises and facilities (physical access control)

Access control to premises and facilities Unauthorized access to premises and facilities must be prevented, whereas the term is to be understood spatially.

Measure	Status
Data processing equipment is under lock (servers hosted in secure data centers)	yes
Adherence to bring your own device policy	yes
Password protection of screens of workstations	yes
Functional and/or time-limited assignment of user authorizations	yes
Use of individual passwords	yes
Automatic locking of user accounts after multiple incorrect password entries	yes
Automatic password-protected screen locking after inactivity (screen saver)	yes
Minimum of 8 characters / upper and lower case, special characters, numbers (of which at least 3 criteria)	yes
Prevention of trivial passwords	yes
Password history (no re-use of the last 5 passwords)	yes
Hashing of stored passwords	yes
Hashes are added with a “Salt” or “Pepper”	yes
Procedure for the assignment of authorizations with the entry of employees	yes

Measure	Status
Procedure for revocation of authorizations due to department change of employees	yes
Procedure for revocation of authorizations due to exit of employees	yes
Obligation to confidentiality / data secrecy	yes
Logging and regular evaluation of system usage	yes
Controlled destruction of data carriers	yes

1.2 Access Control to Systems (Hardware access control)

Access control to systems The intrusion of unauthorized persons into the data processing systems or their unauthorized use must be prevented.

Measure	Status
Data processing equipment is under lock (e.g. closed cage for servers)	yes
Adherence to bring your own device policy	yes
Password protection of screens of workstations	yes
Functional and/or time-limited assignment of user authorizations	yes
Use of individual passwords	yes
Automatic locking of user accounts after multiple incorrect password entries	yes
Automatic password-protected screen locking after inactivity (screen saver)	yes
Minimum of 8 characters / upper and lower case, special characters, numbers (of which at least 3 criteria)	yes
Prevention of trivial passwords (e.g. Dog1, Dog2, Dog3)	yes
Password history (no re-use of the last 5 passwords)	yes
Hashing of stored passwords	yes
Hashes are added with a “Salt” or “Pepper”	yes
Procedure for the assignment of authorizations with the entry of employees	yes
Procedure for revocation of authorizations due to department change of employees	yes
Procedure for revocation of authorizations due to exit of employees	yes
Obligation to confidentiality / data secrecy	yes
Logging and regular evaluation of system usage	yes
Controlled destruction of data carriers	yes

1.3 Access control to Data (software access control)

Access control to data Unauthorized activities in data processing systems outside of assigned authorizations must be prevented.

Measure	Status
Definition of access authorization, authorization concept	yes
Procedure for the recovery of data from backups (who, when, on whose request)	yes
Regular review of authorizations	yes
Restriction of free and uncontrolled query options for databases	yes
Regular evaluation of logs (log files)	yes
Partial access to data stocks and functions (Read, Write, Execute)	yes
Use of appropriate security systems (software/hardware): Virus scanner	yes
Use of appropriate security systems (software/hardware): Firewalls	yes

1.4 Separation Control

Separation control Data collected for different purposes must also be processed separately.

Measure	Status
Separation of customer data (multi-client capability of systems)	yes
File separation in databases	yes
Logical data separation (e.g. based on customer or client IDs)	yes
Authorization concept that takes into account a separate processing of data of different customers	yes
Separation of functions	yes
Separation of development, test and production system	yes

1.5 Pseudonymisation (Art. 32 para. 1 lit. a GDPR; Art. 25 para. 1 GDPR)

The processing of personal data in such a way that the data can no longer be attributed to a specific data subject without further information, provided that such additional information is kept separately and subject to appropriate technical and organizational measures.

Measure	Status
Measures:	n/a

2. Integrity (Art. 32 para. 1 lit. b GDPR)

2.1 Control of transmission

Control of transmission Aspects of the transfer (transmission) of personal data are to be regulated: electronic transfer, data transport as well as their control.

Measure	Status

Measure	Status
What is the mode of transmission of data between Controller and third parties?	
Data exchange via https connection	yes
Encryption of data carriers with confidential data	yes
Encryption of laptop hard disks	yes
Controlled destruction of data	yes
No use of physical data carriers	yes
No use private data carriers at work	yes
Paper disposal: Secure destruction of paper documents	n/a
Juicer is a paperless organization	yes

2.2 Entry control

Entry control Traceability and documentation of data administration and maintenance must be guaranteed.

Measure	Status
Labelling of collected data	yes
Definition of user authorizations (profiles)	yes
Differentiated user authorizations: Read, modify, delete	yes
Partial access to data or functions	yes
Logging of entries / deletions	yes
Obligation to confidentiality / data secrecy	yes

3. Availability and Resilience (Art. 32 para. 1 lit. b GDPR)

3.1 Availability control

Availability control The data must be protected against accidental destruction or loss.

Measure	Status
Data protection and backup concept	yes
Carrying out data protection and backup concept	yes
Restriction of access to server rooms to authorised personnel	yes
Fire alarm systems in server rooms	yes
Smoke detectors in server rooms	yes
Waterless firefighting systems in server rooms	yes
Air-conditioned server rooms	yes
Lightning / overvoltage protection	yes

Measure	Status
Water sensors in server rooms	yes
Server rooms in separate fire compartments	yes
Keep backup systems in separate rooms and fire compartment	yes
Ensure technical readability of backup storage media for the future	yes
Storage of archive storage media under necessary storage conditions (air conditioning, protection requirements, etc.)	yes
CO2 fire extinguishers in the immediate vicinity of the server rooms	yes
Agreement regarding transfer of the (data) backups	yes
Emergency plan (e.g. water, fire, explosion, threat of attacks, crash, earthquake)	yes
Vulnerability analysis (terrain protection, building protection, intrusion into computers, computer networks)	yes
Storage of data in data storage cabinets, safes	yes
UPS system (uninterruptible power supply)	yes
Power generator	yes

3.2 Resistance and reliability control

Resistance and reliability control Systems must be able to cope with risk-related changes and must be tolerant and able to compensate disruptions.

Measure	Status
Alternative data centers available (Hot- or Cold-Stand-by?): Hot	yes
Redundant power supply	yes
Redundant UPS system	yes
Redundant power generators	yes
Redundant air conditioning	yes
Redundant fire fighting	yes
Other redundant systems / procedures: Hard disk mirroring	yes
Computer Emergency Response Team (CERT)	yes
Loadbalancer	yes
Data storage on RAID systems (RAID 1 and higher)	yes
Delimitation of critical components	yes
Performance of penetration tests	yes
System hardening (deactivation of non-required components)	yes
Security is included as a main consideration during the design phase of the systems	yes
Definition of security measures to protect and validate communication between	yes

Measure	Status
system components	
Limitation of authorizations on a need-to-know basis	yes
External contractors (service providers) and maintenance personnel must have a specific access, which must only be active during the intervention and remain disabled the rest of the time	yes
Periodic security training and awareness campaign within the organization	yes
Awareness campaigns to inform users of the security concepts of specific systems and traditional IT systems	yes
Specific security training to teach how to apply security measures and behaviors on the daily processes with the least impact possible	yes

4. Procedures for regular testing, assessing and evaluating (Art. 32 para. 1 lit. d GDPR; Art. 25 para. 1 GDPR)

4.1 Control procedures

Control procedures A procedure is to be implemented for regularly testing, assessing and evaluating the effectiveness of the data security measures.

Measure	Status
Records of processing activities are reviewed and at least updated annually (where applicable)	yes
Notification of new/changed data processing procedures to the Data Protection Officer	yes
Notification of new/changed data processing procedures to the IT Security Officer	yes
Processes for reporting new/changed procedures are documented	yes
Privacy-friendly settings are selected	yes
Security measures are subject to regular internal audits	yes
In the event of a negative outcome of the above-mentioned review, the security measures are adjusted, renewed and implemented in line with the risks involved	yes
There is a process to prepare for security breaches (attacks) and system failures as well as to identify, contain, eliminate and recover them (incident response process)	yes

4.2 Control of instructions

Control of instructions It must be ensured that commissioned data processing by service providers (subcontractors) is only processed in accordance with the instructions of the Processor.

Measure	Status
Contracts according to the requirements of Art. 28 GDPR	yes
Centralized registration of commissioned service providers (contract management)	yes
Regular monitoring of the technical and organizational measures taken by the service providers (during contract period)	yes
On-site inspection at the services providers' premises and facilities	yes
Auditing of the contractor's data security concept	yes
Inspection of existing IT security certificates of contractors	yes

Annex 2

Approved subcontractors

The Controller agrees to the commissioning of the following subcontractors, but only under the condition of a contractual agreement in accordance with Sections Art. 28 para. 2-4 GDPR:

Company (subcontractor)	Processing site	Type of service
Sinch (Mailgun, Mailjet)	USA	Email Marketing Services
Customer.io	USA	Email Marketing Services
Salesforce (Heroku)	USA	Hosting and Infrastructure Services
Amazon	USA	Hosting and Infrastructure Services
Digital Ocean	EU, USA	Hosting and Infrastructure Services
Mixpanel	USA	Tracking and Analytics Services
Hotjar	EU, USA	Tracking and Analytics Services
Talend (Stitch)	USA	Analytics Services
Stripe	USA	Payment Processing Services
Helpwise	USA	Customer Support and Communication Services
Intercom	USA	Customer Support and Communication Services
HubSpot	EU	Customer Relationship Management
Churnkey	USA	Subscription management
Mezmo	USA	Log aggregation & analysis
Cloudflare	USA	DNS and CDN Services
Google Workspace	USA	Business productivity

Company (subcontractor)	Processing site	Type of service
Slack	USA	Collaboration and Communications
Zapier	USA	Automation