Impossible Cloud

Data Processing Agreement
Article 28 GDPR

Status: June 2025

Data Processing Agreement between

Impossible Cloud GmbH
Friesenweg 12
22763 Hamburg, Germany
- Processor, hereinafter referred as **"the Agent"-**

and

- Controller, hereinafter referred as **"the Principal"**-

Principal and Agent individually designated as "Party" and collectively as "Parties".

1. Subject-Matter

In the framework of the delivery and performance relationship between the parties (hereinafter referred to as the "Main Agreement") it is necessary that the Agent handles personal data as a processor in the sense of Article 4 no. 8 GDPR, for which the Principal is responsible as controller or processor of the controller in the sense of Article 4 no. 7 GDPR (hereinafter referred to as "Principal-Data"). This Agreement concretizes the data privacy rights and duties of the parties in the context of handling the Principal-Data for the performance of the Main Agreement by the Agent.

As GDPR best practices evolve, the Agent reserves the right to amend or supplement this Agreement at any time, provided such changes are reasonable for the Principal, considering the Agent's interests (§§ 305 ff. BGB). The Agent will notify the Principal of material changes in text form, granting a reasonable prior notice period. The Principal may object to such changes on reasonable grounds within two weeks of notification (§ 305b BGB). The Agent will inform the Principal of this two-week objection period and the requirement for reasonable grounds for objection upon notification. If the Principal does not object within this period, the changes are deemed accepted (§ 305b BGB). In case of a justified objection, the Agent may either continue services under the prior terms or terminate the Main Agreement with two weeks' written notice (§ 305c BGB).

2. Nature and Purpose of the Processing, Nature of the Personal Data, Categories of Data Subjects, Duration of the Processing

The Agent shall process the Principal-Data for the duration of the contract on behalf of and in compliance with the instructions of the Principal. The Principal remains the controller according to Article 5 (2) GDPR . Nature and purpose of the processing as well as the nature of the personal data and the categories of data subjects are specified in Annex 1. The type of data and categories of data subjects that are being processed by the Agent is determined by the Principal. The Agent shall not process any personal data deviating from or going beyond this, in particular if it's for the Agents' own purposes.

3. Principal's Rights to Give Instructions

3.1. Instructions from the Principal shall be given in writing or text form (e-mail being sufficient).

3.2. The Agent shall carry out the instructions of the Principal without undue delay or, where applicable, in compliance with a reasonable deadline set by the Principal. The Agent shall, in particular, rectify, delete and block personal data as instructed by the Principal without undue delay and confirm this in writing upon request.

3.3. If the Agent considers that an admissible individual instruction violates applicable provisions of the General Data Protection Regulation or other data privacy provisions of EU law or the law of the Member States, the Agent shall point this out to the Principal without undue delay. The Agent is entitled to suspend the execution of the instruction until the instruction is confirmed by the Principal.

3.4 If the Processor is obligated by Union or Member State law to process personal data without the Controller's instructions, the Processor will inform the Controller of the reason for the processing and the corresponding legal requirements prior to the processing, unless such notification is prohibited for important public interest reasons.

4. Duties of the Principal

4.1. The Principal shall be externally, i. e. vis-à-vis third parties and data subjects, responsible for the lawfulness of the processing of the Principal-Data and for safeguarding the rights of data subjects.

4.2. The Principal shall keep all business secrets of the Agent (in particular those with regard to technical and organisational measures) acquired in the context of the contractual relationship confidential. This obligation shall remain in force even after termination of this contract.

4.3. Insofar as the Agent defends himself with legal means against a claim for damages according to Article 82 GDPR, against an imminent or already imposed administrative fine according to Article 83 GDPR or other sanctions in the sense of Article 84 GDPR, the Principal shall allow the Agent to disclose details of the processing for the purpose of legal defense, including instructions issued from the Principal.

5. Duties of the Agent

5.1. If a data subject addresses the Agent directly in the exercise of his rights under Chapter 3 GDPR (Art. 12-23 GDPR), taking into account Part 2, Chapter 2 BDSG (Sections 32-37 BDSG), the Agent shall immediately forward this request to the Principal and support the Principal in a reasonable manner with appropriate technical and organisational measures to comply with his obligation to respond to such requests for the exercise of the rights of the data subject specified in Chapter 3 DSGVO.

5.2. The Agent shall support the Principal in complying with the duties arising out of Art. 32-36 GDPR taking into account the nature of the processor and the information available to the Agent.

5.3. If the Agent becomes aware of a personal data breach within the meaning of Art. 4 No. 12 GDPR it shall immediately notify the Principal thereof. Within this notification pursuant to Art. 33 para. 2 DSGVO, the Agent shall inform the Principal as comprehensive as possible about the nature and extent of the incident and the time it occurred, the IT system and data subjects affected, the time of discovery, all conceivable adverse consequences of the personal data breach and the measures taken as a result.

5.4. The Agent informs the Principal without undue delay if the rights of the Principal concerning the personal data held by the Agent are significantly affected by measures taken by third parties or other events.

5.5. The Agent shall return or delete all Principal-Data at the request of the Principal. Copies and duplicates of the personal data may only be made with the prior consent of the Principal, unless they are used for the proper execution of this agreement or the respective project assignment or to comply with legal storage obligations.

5.6. If the Agent is legally required, it shall assign a data protection officer (Art. 37-39 GDPR). His or her contact details and where applicable information about his or her replacement shall be given to the Principal for the purpose of direct contact at least in text form (e-mail being sufficient).

6. Security in the Processing

6.1. The Agent shall take all measures necessary pursuant to Art. 32 GDPR to grant a level of data security commensurate with the risk of processing. In particular, these measures include the ability to restore the confidentiality, the integrity, the availability and the resilience of the systems permanently and to restore the availability of and access to personal data quickly after a physical or technical incident.

6.2. The Agent shall implement the technical and organisational measures listed in **Appendix 2** prior to commencing the processing of Principal-Data, and maintain them for the duration of the processing and to adapt them commensurate with the state of the art and the risk of the processing. The Agent ensures that the TOMs are updated as part of the regular evaluations, especially with regard to new risks and technological developments.

6.3. The Agent shall guarantee that all individuals authorized to process personal data are bound by a duty of confidentiality or are subject to applicable legal obligations of confidentiality, and shall further guarantee that said processing of personal data is limited to the extent strictly necessary for the execution, administration, and oversight of the contract.

7. Supervision Authority of the Principal

7.1. The Agent shall grant the Principal the right to evaluate the data processing and the compliance with this contract or the respective project assignment. In particular, the Agent shall provide the Principal with all information required to prove compliance with the obligations laid down in this Agreement and shall enable the execution of evaluations, including inspections.

7.2. The parties agree that the Principal shall conduct an evaluation in accordance with Clause 7.1 by instructing the Agent, at the Agents' option, to submit an appropriate audit report, a report or extracts of reports from independent bodies (e.g. accountants, auditors, data protection officers, data protection officers, data protection auditors or quality auditors) or an appropriate certification by an IT security or data protection audit. Notwithstanding, the Principal may conduct an independent evaluation when reasonably justified.

7.3. The Agent shall support the Principal in its evaluation. This includes granting the Principal all access, information and inspections rights. The same applies to evaluations conducted by the competent supervisory authority in accordance with the applicable data protection regulations.

7.4 The Principal shall inform the Agent about all circumstances relating to the conduct of the evaluation in due time (generally at least four weeks prior to the evaluation). Generally, the Principal may conduct an evaluation no more than once per calendar year. Notwithstanding the foregoing, the Principal shall have the right to conduct further evaluations in the event of special occurrences.

8. Subprocessors

8.1. The Agent may subcontract with further processors (subprocessors). For the time being, the Agent commissions the subcontractors listed in **Appendix 3**. The Principal agrees to their commissioning. The Agent shall inform the Principal of any intended change in relation to the use or replacement of subcontractors, which shall give the Principal the opportunity to object to such changes within two weeks, although this may not be done without good cause in terms of data protection law. Unless the Principal raises justified objections within two weeks of notification of the change, the change shall be deemed to have been approved by the Principal. In the event of an objection, the Agent has the option to provide the service without the proposed change. Alternatively, if the Agent considers that providing the service without the intended change is not a reasonable course of action, either the Agent or the Principal may terminate the Main Agreement by giving two weeks' prior written notice.

8.2. Should the commissioning of a subprocessor lead to a transfer of Principal-Data to a country outside of the European Union (EU) or the European Economic Area (EEA) ('third country'), clause 9 of this agreement applies.

8.3. The Agent shall ensure that the data protection obligations stipulated in this Agreement also apply vis-à-vis the subcontractor. The Agent shall oblige the subprocessor respectively pursuant to Art. 28 (4) GDPR by way of a contract or another legal instrument in accordance with EU law or the law of the respective member state prior to the commencement of the processing, whereby, in particular, sufficient guarantees must be provided that the appropriate technical and organisational measures are conducted in such a way that the processing complies with the regulations of the GDPR.

9. Transfer of Principal-Data to Third Countries

9.1. Generally, the data processing contractually agreed upon shall be conducted in a member state of the European Union (EU) in a signatory state of the Agreement on the European Economic Area (EEA). Any transfer of Principal-Data to a country outside the EU/EEA ("third country") shall only take place if the special requirements of Art. 44 et seq. GDPR are met.

10. Return and Deletion

10.1. The Agent shall return all Principal-Data after having finished the processing agreed on and, in particular after the end of the contractual performance (in particular in the event of termination or other end of the Main Agreement) and subsequently delete this data in accordance with the applicable regulations (including existing copies). The same applies to test and usage result material and data pertaining to the contractual relationship that have come into its possession. This shall not apply provided Union or Member State law requires storage of the personal data.

10.2. Data and documentation that serves as proof of data processing in accordance with the Main Agreement shall be retained by the Agent beyond the end of the Agreement in accordance with the respective retention periods.

10.3 The Main Agreement may include certain features and functions that allow the Principal to delete, export or copy all of the data being processed by the Agent at any time during the Term of the Main Agreement. In the event of all the data being deleted by the Principal, the Agent will, and will require its Sub-processors to: (a) stop Processing personal data except as otherwise instructed by the Principal; and (b) securely destroy all or any personal data related to this agreement in its possession or control, which includes deleting Principal's account, after which time Principal will no longer have access to the data uploaded.

10.4 Notwithstanding the foregoing, if there is a legal requirement for the Agent to retain copies of personal data on archive or other back-up media in accordance with its backup or other disaster recovery procedures, the Agent shall notify the Principal in writing of that retention requirement, giving details of the personal data that it must retain, the legal basis for retention, and establishing a specific timeline for destruction once the retention requirement ends.

10.5 Documentations which serve the purpose of proving the orderly and due data processing or legal requirements of record-keeping shall be kept by the Agent according to the respective record-keeping periods beyond the duration of the contract.

11. Duration and Termination

The term and termination of this Agreement shall be governed by the provisions concerning the term and termination of the Main Agreement. A termination of the Main Agreement automatically results in the termination of this Agreement. An isolated termination of this Agreement is excluded.

12. Miscellaneous

Unless special provisions are contained in this Agreement, the provisions of the Main Agreement, including place of jurisdiction, shall apply. In the case of any conflicts between provisions of this Agreement and provisions of other agreements, in particular with the Main Agreement, the provisions of this Agreement shall prevail.

In the event of conflicts between different language versions of this Agreement, the German version shall prevail.

Appendix:

- Appendix 1: Nature and purpose of the processing, Type of personal data, Categories of data subjects
- Appendix 2: Technical and organisational matters
- Appendix 3: Subcontractors

Appendix 1: Nature and Purpose of the Processing, Type of Personal Data, Categories of Data Subjects

1. Nature and Purpose of the Processing

The contractor provides hosting services for the client or customers of the client. The client or its customers determines which content is stored on the provided servers. The contractor has access to this content in order to perform support and maintenance tasks. Additionally, the contractor has access to the log data of the systems. Furthermore, the contractor has access to the data created by the client or customers of the client in the Partner Portal of Impossible Cloud.

2. Type of Personal Data

The processed personal data is determined by the client or customers of the client. The client or its customers can independently utilize the provided storage spaces and upload all information themselves.

Typically, the scope of the contract includes the processing of the following personal data:

- Identification data (e.g., IP address)
- Contact details (e.g., name, email address, phone number)
- Log data

3. Categories of Data Subjects

The categories of affected individuals are determined by the information uploaded by the client or its customers. Typically, the following groups of individuals are affected:

- Customers of the client
- Employees of the client or its customers
- Service providers and other business partners of the client or its customers

Appendix 2: Technical and Organisational Measures

1. **Confidentiality (Article 32 (1) Pt. b GDPR) and Encryption (Article 32 (1) Pt. a GDPR)**

Organisational

- Role-based access controls (RBAC) for data and system access.
- Multi-Factor Authentication (MFA) for administrative and privileged accounts.
- Employee confidentiality agreements and background checks where applicable.
  Security and GDPR awareness training conducted annually for all staff.
- Data Processing Agreements (DPAs) signed with all third-party vendors.
- Due diligence review of third party suppliers (Vendors) security practices, inc. security compliance certifications, audit reports and contractual documentation.

Technical

- Electronic Control and Data Encryption:
    - AES-256 encryption for data at rest (on all storage volumes and backup systems) and HTTPS protocol.
    - TLS 1.2+ encryption for data in transit across internal and external networks.
    - End-to-end encryption design for distributed data flow.
    - cryptographic protection encryption algorithm SHA-256.1 and similar
    - support of server-side encryption (SSE). The SSE options include SSE-S3 (using AES256 encryption - X-Amz-Server-Side-Encryption: AES256) and SSE-C (customer-based key - X-Amz-Server-Side-Encryption-Customer-Key). Customers can specify the SSE parameters using a S3 client application when writing objects to buckets. With the encryption key a customer provides as part of their request, Impossible Cloud manages the encryption as it writes to disks and decryption when customers access their objects. Customers must manage the encryption keys they provide. An access key is for use with third-party applications and is used to make programmatic calls to AWS API actions. Customers must use two types of access keys: Access Key ID and Secret Access Key. Impossible Cloud does not access or view a customer's secret key as part of providing the Service. A customer's Access Key ID can be visible to IC support staff.

- IAM & Key Management:
    - IAM enforced via centralized directory and strict access provisioning to manage S3 permissions: IAM policies specify which user can access specific buckets and objects.
    - Secure key management.
    - Enablement of key rotation
    - audit logging of key usage.

- Physical Access Controls at third parties facilities:
    - Access to physical hardware restricted to named, authorized personnel only.
    - Secure and tamper-evident racks in certified third-party data centers.

    - Biometric, badge-based, and escorted access controls at third-party facilities.

- Vendor Controls:

    - Selection limited to SOC 2 and ISO 27001-certified or equivalent facilities within EU.
    - Metadata is distributed and stored in Tier 3 Datacentres.

- Impossible Cloud IT Systems and Network Access Control:

    - Two-factor authentication for most critical IC IT systems.
    - Network segregation and firewall with ACL rules and subnet services to prevent unauthorized external access..
    - All servers, DNS servers and Network devices (firewalls, routers, switches…) protected with hardening practices.
    - Access to IT systems is only possible with a user ID and individual password.
    - Access permissions are documented.
    - Functional assignment of individual end devices and logging of system usage for critical events.
    - Avoidance of the use of mobile storage devices.
    - Screen lock on workstations, automatic locking after extended periods of absence.
    - Careful selection of cleaning personnel.
    - Dedicated Teleworking Policy for All Employees for the Implementation of Mobile Work

- Internal Access Control:

    Personnel who has access to data processing is subject to additional control measures:

    - access granted based on job responsibilities
    - Individual access rights and segregation of for each user (documented in a written authorization concept), centrally managed and controlled by system administrators.
    - Dedicated permissions per user role for IT systems for reading, editing, and deleting.
    - Regular review of access permissions. Unnecessary permissions are revoked promptly.
    - Recording of accesses to the IT system.
    - Definition of user roles and corresponding assignment of stakeholders.
    - Logging of access, editing, and deletion of files

- Separation Control
    - Separation of production and test systems.

Access permissions are task-based and limited to a minimum. This also applies to the number of administrators. External contractors never access production data.

2. Integrity (Art. 32 (1) Pt. b GDPR)

SSE S3 can be enabled by the Principal, therefore the Principal is responsible for encrypting their own data.

Organisational

- Use of on site physical storage media is prohibited.
- When hardware is circulated or exchanged, hard drives are wiped and reinstalled.
- Visitors do not have access to the operational LAN/WLAN.
- Changes to the system landscape requires approval or review by at least two qualified employees
- Employee training on phishing attempts and general dangers related to email usage.

Technical

- Checksums and digital signatures are used to verify data integrity across Hardwares
- Replicas and erasure code minimises the corruption of data and allows eleven 9s object durability
- Immutable logging systems (SIEM) in place for capturing data access and modifications.
- File integrity monitoring

3. Availability and Resilience (Art. 32 (1) Pt. b GDPR), Rapid Recovery (Art. 32 (1) Pt. c GDPR)

Organisational

- Dedicated data security concept ("Information Security Policy").
- Protection against malicious software (malware).
- Dedicated reporting procedure and dedicated incident response plan ("Data Breach Response Plan").

Technical

- Distributed Storage Architecture:
    - Data is segmented and replicated across multiple servers for resilience.
    - Load balancing and health checks ensure high availability and fault tolerance.
- Third-Party Data Center Measures:
    - Use of Tier III+ or ISO 27001-certified data centers with redundant power, cooling, and connectivity.
    - 24/7 surveillance and physical protection measures (CCTV, security guards, biometric entry).
- Disaster Recovery and Backup:

    - Encrypted backups performed regularly
    - Disk mirroring (RAID) for Internal DBs
    - Erasure coding for customers data.

- Dedicated data security concept for metadata ("Information Security Policy").

    - Versioned data and system backups according to a backup plan
    - Disk mirroring (RAID).
    - Protection against malicious software (malware).
    - Security-related updates and patches are applied regularly and promptly.
    - Dedicated reporting procedure and dedicated incident response plan ("Incident Response Plan").

4. Procedures for Regular Testing, Assessment and Evaluation (Art. 32 (1) Pt. d GDPR; Art. 25 (1) GDPR)

Organisational

- Contract and Agreement Control
- DAP and NDA signed with any third party engaged into Testing, Assessment and Evaluation
- Training to third Parties employees in data protection and awareness in data confidentiality
- Data-protection-friendly default settings are taken into account for software development
- Employees are regularly instructed in data protection law and are familiar with the procedural instructions and user guidelines for data processing on behalf of the Client also with regard to the Client's right of instruction.
- A company Data Protection Officer and an Information Security Officer are appointed and integrated into the relevant operational procedures.

Technical

- Regular penetration tests by certified third-party security firms.
- Annual audits including GDPR DPAs.
- Privacy-by-Design and Security-by-Design reviews integrated into the software development lifecycle (SDLC), including:

    - Mandatory privacy impact checks

5. Pseudonymisation (Art. 32 (1) Pt. a GDPR, Art. 25 (1) GDPR

Measures to ensure that personal data is processed in such a way that the data cannot be associated to a specific concerned person without the assistance of additional information, provided the additional information is stored separately and is subject to appropriate technical and organisational measures:

- Personal data is modified or aggregated in such a way that it can no longer be directly attributed to a specific individual.
- Personal data is separated from other data and stored separately to facilitate pseudonymization.
- Personal data is restricted to a regional level, ensuring, for example, that access to personal data from the EU or authorised third countries is not possible.

Appendix 3: Sub-processors

Within the scope of the Main Agreement, there are currently no service providers who have access to or process data uploaded by the Principal, as sub-processors of the Agent.