Data Processing Agreement (DPA)

pursuant to Art. 28 GDPR · Version 1.0, June 2026

This Data Processing Agreement ("DPA") forms an integral part of the Terms & Conditions ("Agreement") between TechnologyCircle GmbH and the Customer and governs the processing of personal data by TechnologyCircle GmbH in connection with the CustomJS service.

Processor
TechnologyCircle GmbH
Karolinenstraße 24, Haus 4
20357 Hamburg, Germany
Operator of: CustomJS
Represented by: Henrik Lippke, Managing Director
Email: info@technologycircle.io

Controller
The Customer, the natural or legal person who registers for and/or accepts the Agreement. The Customer acts as Controller (or itself as processor on behalf of a third-party controller) for the personal data processed via the Service.

Conclusion and Form
This DPA is concluded upon the Customer's acceptance of the Agreement / registration for the Service. No signature is required; it is concluded in electronic form pursuant to Art. 28(9) GDPR.

Section I, General

Clause 1, Purpose and Scope
This DPA ensures that the processing of personal data on behalf of the Controller by the Processor is carried out in accordance with Article 28(3) and (4) GDPR.

Clause 2, Non-alterability
The DPA may only be amended to supplement the annexes, without altering fundamental provisions.

Clause 3, Interpretation
Terms are interpreted in accordance with the GDPR.

Clause 4, Precedence
In the event of a conflict regarding data protection, the provisions of this DPA shall prevail. In all other respects, the Agreement (Terms & Conditions) governs.

Section II, Obligations of the Parties

Clause 5, Description of Processing
The subject matter, nature, purpose, data categories and duration of the processing are set out in Annex II.

Clause 6, Obligations of the Processor
6.1 Instructions: Processing shall only be carried out based on documented instructions from the Controller. The Controller's documented instructions are set out in this DPA, the Agreement, and the Customer's configuration and use of the Service; the Customer's use of the Service constitutes such instruction. This includes instructions regarding transfers to a third country, unless the Processor is

required to transfer by Union or Member State law.

6.2 Purpose limitation: Processing only for the purposes listed in Annex II.

6.3 Duration: As defined in Annex II.

6.4 Confidentiality: The Processor ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality. The Processor treats all personal data and non-public information of the Controller as confidential and uses it solely to provide the Service.

6.5 Security of Processing (Art. 32 GDPR): The Processor implements appropriate technical and organizational measures as specified in Annex III. The parties periodically review and update these measures to reflect the current state of the art.

6.6 Sensitive data: Not applicable (see the data restriction in Annex II).

6.7 Accountability: Both parties shall provide each other with all information necessary to demonstrate compliance with Art. 28 GDPR.

6.8 Sub-processors: The Controller grants a general written authorization for the engagement of sub-processors. The current list of sub-processors is available at https://www.customjs.space/subprocessors. The Processor shall inform the Controller of any intended addition or replacement of sub-processors, giving the Controller the opportunity to object. The Processor imposes the same data protection obligations on each sub-processor (Art. 28(4) GDPR).

6.9 International Data Transfers: Where personal data is transferred to the United States, such transfers are based on the EU-U.S. Data Privacy Framework (adequacy decision) or, where applicable, the EU Standard Contractual Clauses (SCCs). Details in Annex IV.

6.10 Audit and Inspections: The Processor shall make available all information necessary to demonstrate compliance with Art. 28 GDPR and allow for and contribute to audits, including inspections, by the Controller or a mandated auditor. Audits shall take place during regular business hours, following reasonable prior notice (at least 14 days), and shall not unreasonably interfere with the Processor's operations.

Clause 7, Assistance to the Controller

The Processor shall assist the Controller in handling data subject requests and in conducting data protection impact assessments, taking into account the nature of the processing and the information available to the Processor.

Clause 8, Notification of Data Breaches

The Processor shall notify the Controller of any personal data breach without undue delay, and in any event within 48 hours after becoming aware of it. The notification shall include the information required by Art. 33(3) GDPR to enable the Controller's reporting obligation.

Section III, Final Provisions

Clause 9, Termination

Upon termination of the Agreement, the Processor shall, at the choice of the Controller, delete or return all personal data, and confirm deletion in writing upon request. This includes data stored in backups, which is deleted in accordance with the Processor's regular deletion cycle (and put beyond use in the meantime).

Annex I, List of Parties

Processor: TechnologyCircle GmbH, Henrik Lippke (Managing Director), info@technologycircle.io

Controller: The Customer, as identified by the account / registration data provided to the Service.

Annex II, Description of Processing

Categories of Data Subjects: Users of the Controller's services and any individuals whose data is included in the processed content.

Categories of Data:

- *Agnostic Content Data:* Any personal data provided dynamically by users for PDF generation or JS execution (e.g. identity, contact, or transaction data within HTTP requests).
- *Technical Metadata:* IP addresses and logs necessary for the execution of the services.

Data Restriction (the "Agnostic" Safeguard): The Service is a content-agnostic processing tool. The Controller shall not use the Service for special categories of personal data (Art. 9 GDPR) or data relating to criminal convictions (Art. 10 GDPR). The Processor is not required to monitor content; responsibility for ensuring that no sensitive data is submitted rests solely with the Controller and its end-users.

Nature of Processing:

- Receipt of incoming HTTP requests for real-time PDF generation and JS execution
- Temporary (volatile) storage only for the duration of processing
- Generation of execution logs

The Processor has no routine access to the content of customer logs. Access is strictly limited to automated system-level monitoring and troubleshooting by authorized personnel, subject to the confidentiality obligations in Clause 6.4. No data mining, profiling, or processing beyond documented customer actions.

Purposes: Automation services such as PDF generation, screenshot creation, and JavaScript execution on behalf of the Customer.

Duration: For the duration of the contractual relationship / the Customer's use of CustomJS.

Annex III, Technical and Organizational Measures (TOMs)

- Access control through IAM roles
- Logging of security-relevant activities
- AWS Security Hub for continuous monitoring
- TLS encryption in transit
- AES-256 encryption of data at rest
- Restricted access to trained personnel
- Systematic pseudonymization and data minimization

Annex IV, List of Sub-Processors

The current list is maintained at https://www.customjs.space/subprocessors. As of the last update:

1. **Amazon Web Services EMEA SARL / AWS Ireland Services Ltd.** Region: AWS EU (Frankfurt). Infrastructure (hosting, data processing).

2 **Amazon Web Services, Inc. (USA)** Support & administration. Transfer mechanism: primarily the EU-U.S. Data Privacy Framework (AWS is actively DPF-certified); EU SCCs as a fallback.

Transfer Impact Assessment: Primary storage and processing is in Frankfurt (Germany); data is encrypted at rest (AES-256) and in transit (TLS); the Service allows no sensitive data; the US entity is subject to the DPF. The parties conclude that the safeguards are sufficient and the residual risk to data subjects is negligible.

This DPA is concluded electronically in accordance with Art. 28(9) GDPR and requires no signature. Version 1.0, June 2026.