



CLEVERBRIDGE THIRD PARTY TOOL IMPLEMENTATION AND USAGE TERMS

Client requests that Cleverbridge implement or allow Client to implement a Cleverbridge-approved Third Party Tool onto the Cleverbridge Online Store. Client agrees it will use the approved Third Party Tool(s) in accordance with these Implementation and Usage Terms along with the [Cleverbridge Acceptable Conduct Policy](#) and the [Client Security Requirements](#) (both found at grow.cleverbridge.com/legal-info) and the Data Processing Agreement found in Annex A (collectively including these terms, annexes and policies, the “**Terms**”). Noncompliance with these Terms may result in Cleverbridge, at its discretion, disabling the Third Party Tool and/or removing it from the Cleverbridge Online Store. These Terms are further subject to the terms of the signed Cleverbridge Reseller Agreement or Cleverbridge Master Subscription Agreement between the parties (the “**Agreement**”). Any capitalized terms not defined herein shall have the meaning defined in the Agreement.

Approval of Third Party Tools

All Third Party Tools must be approved in writing by Cleverbridge. Client’s use of any Third Party Tool(s) on the Online Store not explicitly stated herein, or not otherwise approved in writing by Cleverbridge, is strictly prohibited. Requests to use a Third Party Tool not listed in these Terms may be sent to your Cleverbridge Client Success Manager.

Client agrees that Cleverbridge must implement and operate a layered consent solution within the Cleverbridge shopping cart including a cookie banner to collect informed consent from users on behalf of the Client.

Security Settings

Client will, to the extent offered by a Third Party Tool, implement one of the following methods to authenticate all users accessing the Third Party Tool:

1. 2-factor authentication; or
2. Password or passphrase that has a minimum length of eight characters, contains both numeric and alphabetic characters, and needs to be changed at least every 90 days.

Impact on the Cleverbridge Online Store

Client will not use Third Party Tools to alter any portion of the e-commerce checkout process or elements of the Cleverbridge Online Store, including, but not limited to, links to Cleverbridge Terms & Conditions or Privacy Policy.



Requirements by Tool Type

1. Pop-ups: Client will implement any pop-up windows/ “Don’t Leave Layers” as follows:
 - a. give customers the opportunity to leave the window as easily as it is for them to accept the offer.
 - b. provide a link to the Client’s privacy policy prominently within the pop-up window.
2. Chat Tools: Client will make clear that the chat is operated by Client and not by Cleverbridge.
3. Session Recording/ Monitoring and Heatmap Tools: Client will mask or censor all personal data e.g., by enabling a text suppression feature/replacement of any input by an asterisk for all input fields on the Cleverbridge checkout process so that the data the customer enters is not recorded.
4. Approved Tag Manager Tools: These are tag manager tools that have been approved for use by Cleverbridge including, but not limited to, Google Tag Manager and Tealium. Client must allow Cleverbridge read access to their Tag Manager Tool account throughout the entire usage period. Read access can be granted to tracking-support@cleverbridge.com. Client must also configure and adjust Tag Manager Tool settings according to Cleverbridge specifications.

Audit Rights and Data Access Control

Cleverbridge utilizes automatic scanning tools to audit the Cleverbridge Online Store and provide script integrity monitoring. In the event these scanning tools detect anomalies or security risks linked to the Third Party Tool and scripts used by the Client, Cleverbridge will block and restrict the specific scripts from accessing sensitive information, in order to prevent unauthorized script behaviors while maintaining full functionality. If Client feels the restrictions are applied in error, Client agrees to reach out to Cleverbridge at compliance@cleverbridge.com.

Client will provide Cleverbridge with all necessary rights to conduct a regular audit of the Third Party Tool and, where possible, a minimum of “read/review” access rights to the Third Party Tool Admin Console in order to check if the Third Party Tool is being utilized in a manner consistent with the Agreement, applicable law, regulations and industry accepted standards. If Cleverbridge determines, in its sole discretion, that the Third Party



Tool is being utilized in a manner inconsistent with these Terms, applicable law, regulations or industry accepted standards, it will notify Client. In such event, Client shall substantially remedy issues identified by Cleverbridge within 48 hours. Failure to remedy the issues may result in Cleverbridge, at its discretion, disabling the tool and/or removing it from the Cleverbridge Online Store.

Annex A

Data Processing Agreement

This Annex is a Data Processing Agreement ("**DPA**") between Cleverbridge, as processor, and Client as controller. Client's use of the Third Party Tools in the Cleverbridge Online Store is expressly conditioned on Client's consent to the terms of this DPA. Cleverbridge's provision of services under Terms requires access by Cleverbridge to Personal Data for which Client alone determines the purposes and means of the processing or is otherwise the controller under Applicable Data Protection Laws.

1. Additional DPA Definitions

- 1.1. "**Applicable Data Protection Laws**" means any data protection legislation, rules and regulations applicable to the Services, including but not limited to the GDPR.
- 1.2. "**Data Subject**" shall have the same meaning as given in the Applicable Data Protection Laws, i.e., a natural person whose Personal Data is processed under this DPA.
- 1.3. "**EEA**" means the European Economic Area.
- 1.4. "**GDPR**" means Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of Personal Data and on the free movement of such data.
- 1.5. "**Personal Data**" shall have the same meaning as given in the Applicable Data Protection Laws, i.e., any information relating to a Data Subject processed via Third Party Tools.
- 1.6. "**processing**", "**processed**" shall have the same meaning as given in the Applicable Data Protection Laws, including but not limited to collection, use, recording, organisation, structuring, adaptation, retrieval, consultation, modification, storage, disclosure, alignment or combination, restriction, erasure or destruction, and any other activity with respect to personal data.
- 1.7. "**Standard Contractual Clauses**" means the standard contractual clauses adopted by the EU Commission Implementing Decision 2021-914 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council which can be found at <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32021D0914>.
- 1.8. "**Third Country**", "**Third Countries**" means any country outside of EEA.
- 1.9. "**Controller**" means the Client.
- 1.10. "**Processor**" means Cleverbridge GmbH, Tunisstraße 19-23, 50667 Cologne, Germany.
- 1.11. "**Subprocessor**" means any subprocessor engaged by Processor for the processing of Personal Data under this DPA.

2. Subject matter; nature and purpose of processing; duration of processing; type of Personal Data and categories of Data Subjects

This DPA relates to and governs the processing of Personal Data by Cleverbridge to the extent required as part of its services under the Terms on behalf of Client, related to its use

of the Third Party Tools. The duration of processing will be until the earliest of (i) the termination of the Terms, or (ii) the date on which processing is no longer necessary for the purposes of either party performing its obligations under the Terms.

2.1. Data Subjects

Data Subjects means the visitors/users of the Cleverbridge Online Store.

2.2. Categories of Data

Personal Data that may be processed includes data relating to the tracking of the Data Subjects (e.g. which products they bought in the Cleverbridge Online Store or how they otherwise used the Cleverbridge Online Store). Data Subjects are not directly identifiable by Cleverbridge and are indirectly identifiable only by reference to their IP address, cookie identifiers or other online or device identifiers, and browser details, among other potential methods. Cleverbridge would require access to additional information in order to identify Data Subjects.

3. Obligations of the Controller

- 3.1. By entering into the Terms, including this DPA, Client instructs Cleverbridge to process Personal Data to the extent required to provide the services under the Terms. Client will not intentionally instruct Cleverbridge to process Personal Data in a manner that would constitute a breach of Applicable Data Protection Laws.
- 3.2. Client will ensure that any instructions given to Cleverbridge comply with all laws, rules, and regulations applicable in relation to the Personal Data, and that the processing of Personal Data in accordance with Client's instructions will not cause Cleverbridge to be in breach of this DPA, the Standard Contractual Clauses, or the Applicable Data Protection Laws.
- 3.3. Client remains the controller of the Personal Data within the meaning of Applicable Data Protection Laws and will act in compliance with Applicable Data Protection Laws. This also includes responding to Data Subject requests and contacting Cleverbridge to respond as required by Applicable Data Protection Laws.
- 3.4. Client will notify Cleverbridge without undue delay of any errors, security incidents or irregularities (if any) Client gains knowledge of in connection with the processing of the Personal Data by Cleverbridge.

4. Additional Obligations of the Processor

- 4.1. In addition to the obligations set out elsewhere in this DPA, Cleverbridge, as Processor, will Process Personal Data only on documented instructions from Client, including with regard to transfers of Personal Data to a Third Country or an international organisation, unless required to do so by Union or Member State law to which Cleverbridge is subject; in such a case, Cleverbridge will inform Client of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest.

- 4.2. Cleverbridge will ensure that Subprocessors have committed themselves to the same confidentiality required under this DPA or are under an appropriate statutory obligation of confidentiality.
- 4.3. Cleverbridge will assist Client by implementing appropriate technical and organisational measures in order for Client to fulfill its obligation to respond to requests for exercising the Data Subject's rights set forth in the GDPR and for Client to ensure compliance with the obligations pursuant to Articles 32 to 36 of the GDPR.

5. Processing Locations and Standard Contractual Clauses

- 5.1. The countries where Cleverbridge may process Personal Data are: Germany and the United States of America. Specifically, data Processing could take place at the following sites of Cleverbridge and its affiliates: **Cleverbridge GmbH**, Tunisstraße 19-23, 50667 Cologne, Germany; and **Cleverbridge Inc.**, 350 N Clark, Suite 700, Chicago, Illinois, 60654, USA.
- 5.2. Client authorizes Cleverbridge to process Personal Data in the above-listed countries, any EU or EEA country, and any Third Country where the European Commission has decided that the Third Country in question ensures an adequate level of protection for the respective Processing.
- 5.3. Cleverbridge will not transfer the Personal Data to any other Third Country unless the appropriate safeguards and Data Subject's rights enforceability and effective legal remedies are secured, in particular by Cleverbridge entering into the Standard Contractual Clauses (or a legally compliant equivalent thereto) with the Subprocessor on behalf of Client.
- 5.4. In the event of a change in any Applicable Data Protection Laws relating to the countries where an adequate level of data protection exists, the Parties will discuss and agree on an alternative solution permitting Cleverbridge to continue to Process the Personal Data in said countries.

6. Technical and organisational measures

- 6.1. Cleverbridge will maintain a record of all categories of processing activities carried out on Client's behalf to the extent required to enable Client to comply with its obligations under Applicable Data Protection Laws, and require any Subprocessors to do the same.
- 6.2. With regard to Third Party Tools, it is Client's obligation to ensure the implementation and maintenance of appropriate technical and organisational data protection and security measures to ensure the security and accountability of the Personal Data as required under Article 32 of the GDPR. With regard to Cleverbridge personnel having access to Personal Data Processed under these Terms and this DPA, Cleverbridge will also take reasonable steps to ensure the reliability and obligation to confidentiality of any person authorized to Process the Personal Data, and will implement and maintain appropriate technical and



organisational data protection and security measures to ensure the security and accountability of the Personal Data as required under Article 32 of the GDPR. Cleverbridge's Technical and Organizational Measures can be found at <https://grow.cleverbridge.com/legal-info> under "Client Terms, Policies, & Documents."

7. Right to Audit

- 7.1. Cleverbridge will make available to Client all information necessary to demonstrate compliance with the obligations set forth in Article 28 of the GDPR and allow Client to reasonably inspect or audit, at Client's own expense, Cleverbridge's (and its Subprocessors') compliance with this DPA and Applicable Data Protection Laws. For this purpose, Cleverbridge will grant Client, or a third party to be designated by the parties, access to Cleverbridge's business premises during Cleverbridge's regular business hours and, without undue delay, make available all information necessary to demonstrate compliance with this DPA as reasonably requested.
- 7.2. Client will notify Cleverbridge in writing of any such audit or inspection, usually at least 15 business days in advance and at the same time provide a concise audit plan detailing the subject of such audit, the audit timeline, and any information or resources requested. Cleverbridge will ensure that similar provisions are included in its written contracts with Subprocessors. Client agrees that if Cleverbridge can provide an ISAE 3402 Type 1, (SOC1 Type 2), or similar audit report prepared by an independent third party auditor, the rights set forth here will only apply insofar as the subject to be audited is not already covered by such audit report and is required for Client to demonstrate its compliance with Client's obligations related to this DPA.

8. Data Breach Notifications

- 8.1. Cleverbridge will notify Client without undue delay after becoming aware of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or unauthorized access to the Personal Data transmitted, stored, or otherwise processed by Cleverbridge or any of its Subprocessors.
- 8.2. Cleverbridge will take reasonable steps to restore any Personal Data lost as a result of such data breach where it is the result of the acts or omissions of Cleverbridge or its Subprocessors.
- 8.3. Cleverbridge will provide assistance with any of Client's obligations under Applicable Data Protection Laws, including making any notifications to the Data Subjects, supervisory authorities or the public in respect of such breach as reasonably requested by Client.

9. Rights of the Data Subjects

- 9.1. Client has the sole responsibility to provide Data Subjects with the information required under Applicable Data Protection Laws by providing such information to Data Subjects in its privacy or cookie policy as set out in more detail in the Terms.
- 9.2. Client also has sole discretion in responding to the rights asserted by the Data Subjects.

10. Cleverbridge's Right to Engage Subprocessors

- 10.1. Client provides a general authorization to Cleverbridge to engage Subprocessors subject to compliance with requirements at least as strict as the obligations of Cleverbridge set out in this DPA.
- 10.2. Cleverbridge will inform Client of any intended changes to its list of Subprocessors thirty (30) days before a new Subprocessor receives access to Personal Data, thereby giving Client the opportunity to object to such changes on the grounds that the Subprocessor does not meet requirements under Applicable Data Protection Laws. If Client objects, Cleverbridge will attempt to make reasonable accommodations but if the subcontractor is required for subprocessing, then Client's objection will be considered an immediate termination of the Terms and this DPA.
- 10.3. Regarding any transfer of Personal Data to Third Countries, Cleverbridge will enter into the Standard Contractual Clauses with all respective data importers on Client's behalf or otherwise ensure that applicable safeguards for the transfer of Personal Data to Third Countries are adopted by contract.

11. Termination

- 11.1. Upon termination of the DPA, Cleverbridge will return to Client or erase/destroy any files containing Personal Data and certify that this has been done, unless prevented from doing so by applicable laws. Cleverbridge reserves the right to erase Personal Data by aggregating it.
- 11.2. Termination of the DPA shall mean termination of the Terms and vice versa.

12. Limitation of Liability regarding the transfer of personal data

- 12.1 For the avoidance of doubt, each party's liability towards data subjects shall be subject to the statutory provisions, in particular Art. 82 GDPR. Nothing in this section will affect either party's liability towards data subjects.
- 12.2 Cleverbridge's liability towards the Client arising out of or in relation to these Terms, whether in contract or in tort, shall be limited as follows:
 - i. Cleverbridge shall be liable to the Client under statutory provisions in the event of intent, gross negligence, culpable injury to life, body or health, assumption of a guarantee or a procurement risk and in the event of liability under the German Product Liability Act.



ii. Cleverbridge shall furthermore be liable to the Client in the event of a slightly negligent breach of material obligations of this Annex, meaning obligations that (i) enable the fulfillment of this Annex, and (ii) on whose fulfillment the Client generally relies and is entitled to rely. In such event, Cleverbridge's liability shall be limited to the typically foreseeable damage.

iii. The parties agree that the typically foreseeable damage shall be limited to the aggregate amount or resale margin received by Cleverbridge during the twelve-months-period immediately preceding the most recent damaging event, minus any damage payments made by Cleverbridge to Client during that same time period.

iv. Any further liability of Cleverbridge towards Client shall be excluded.

v. To the extent Cleverbridge's liability towards Client is excluded or limited pursuant to the provisions above, the same will apply to the personal liability of the corporate entities, legal representatives, employees and other vicarious agents of Cleverbridge.

vi. With regard to Cleverbridge's liability towards Client arising out of or in relation to this Annex, any amounts paid by Cleverbridge to Client arising out of or in relation to this Annex shall be credited against any liability limit agreed upon in the Agreement.

vii. For the avoidance of doubt, this Section 12 shall, within its scope, supersede any provisions in the Agreement concerning Cleverbridge's liability towards Client.

13. Miscellaneous

13.1. In case of introduction of new or change of existing Applicable Data Protection Laws, including GDPR or local, at the request of any party, the parties will promptly review this DPA and begin good faith negotiations to agree on any changes necessary to bring this DPA to line with the law.

13.2. In case of any discrepancies between this DPA and the Standard Contractual Clause, the relevant provisions of the Standard Contractual Clauses prevail.