

Data Processing Agreement

Between Cookiehub, 6801211090, Hafnargata 55, 230 Reykjanesbær , Iceland, here after referred to as „processor“, and customer here after referred to as „controller“.

This agreement is drafted in accordance with the requirements of Art. 28 of Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), here after referred to as GDPR or the General Data Protection Regulation.

I. Purpose of this agreement

The purpose of these contractual clauses is to specify the obligations that the processor fulfills on behalf of the controller, in relation to the processing activities covered by the contract.

The contracting parties shall be bound by all relevant legal provisions concerning the processing of personal data by them, and in particular the General Data Protection Regulation (GDPR).

When definitions such as personal data, data subject etc. are referred to in this agreement, it is interpreted as in the General Data Protection Regulation.

II. Description of the processing of personal data

The processor is permitted to process, on behalf of the controller, the personal data necessary for him to provide services in the form cookie consent. Cookie consent consist of a banner, displayed on the website of the controller, that allows web users the opportunity to grant consent, modify or reject web cookies that are not deemed necessary for the functioning of the website.

The nature and purpose of the processing activity in question here is further described in Annex 1 of this agreement. The processor is permitted to process the following types of personal data and types of data subjects as described in Annex 1.

III. Jurisdiction

In the event of a dispute, arising in connection with this agreement and the parties are not able to reach a common understanding or otherwise peaceful solution, any litigation that may take place shall be before Icelandic courts.

IV. Transfer of data

The processor does not transfer personal data outside of the EU/EEA area. If such a transfer were to occur, it would only occur in accordance with the conditions and rules set out in the GDPR.

V. Confidentiality

The parties agree to keep this agreement and information received about the other party in connection with this agreement confidential and, unless a lawful reason permits to do so, must not use or disclose any information without the prior written consent of the other party.

VI. Agreement period

This agreement is valid from the time that services, on behalf of the processor, are rendered, and expires after the services are no longer rendered. Services are considered rendered by the processor as stipulated in the service agreement between the processor and the controller.

VII. Obligations of the processor

The processor shall:

1. only process personal data in accordance with the purpose of the processing, according to this agreement
2. only process personal data according to the written instructions of the responsible party, which are attached to this agreement. In cases where the processor believes that the responsible party's instructions are not compatible with the GDPR or other relevant legal provisions concerning the processing of personal data, he must notify the responsible party without delay. The processor shall also notify the responsible party if the processor is obliged by law to transfer personal data to a third country or international organizations, unless legislation prohibits such disclosure.
3. ensure the confidentiality of the processing of the personal data covered by this agreement, and
4. ensure that the employees who have access to personal data in connection with the execution of the contract have signed a confidentiality statement or are bound by law to confidentiality and that they receive appropriate training in the protection of personal data.
5. ensure that devices and tools, products, programs, and services are designed with privacy by design and default as a guiding principle.

6. The processor must comply with the GDPR when processing personal data, and applicable data protection laws as far as they are analogous to the GDPR. In case of conflict between GDPR and other applicable data protection laws the processor adheres to the GDPR.

7. Use of sub-processor

The processor may contract with another party (sub-processor) to carry out certain processing operations. Before the intended changes take effect, both when sub-processors are added and when changes are made to the sub-processors that are already used, or in the case of additions or changes to the current arrangement of processing operations, the processor must inform the controller in writing about the changes. It must specifically state which processing operations the sub-processor intends to undertake, the name and contact information of the sub-processor, together with the date of the contract. The responsible party has 30 days from the day it receives information about a change in the use of a sub-processor to object to it. The use of a sub-processor is only permitted when the responsible party has not objected to it within the time limit.

8. Rights of data subjects to be informed

The controller is responsible for providing the data subject with information about the processing activity before or as soon as processing begins, in accordance with Art. 13 and 14 of the GDPR.

9. Grant of rights to the data subjects

To the extent possible, the processor must assist the responsible party in fulfilling its duty to respond to the inquiries of data subjects due to their rights, such as the right of access, the right to rectification and erasure, the right to restrict processing, the right to data portability and the right not to be subject to a decision based solely on automated processing.

When the data subject submits a request to exercise his rights with a processor, the processor must forward such a request without delay to the controller.

This assistance grants the processor the right to charge fees. The controller may inquire about the amount of fees at any given time. The processor will not exercise the right to charge fees unless notifying the controller in advance.

10. Notice of security breach

The processor must notify the controller by email to the email address: _____, of any type of security breach no later than 24 hours after becoming aware of the breach. The notice must be accompanied by all the documents or data that are necessary for the controller to report the security breach to the relevant supervisory authority.

11. Assistance towards the controller in fulfilling the conditions of the General Data Protection Regulation

The processor shall assist the controller in carrying out a Data Protection Impact Assessment (DPIA).

The processor shall assist the controller in fulfilling the provisions of the GDPR on prior consultation with the relevant supervisory authority.

This assistance grants the processor the right to charge fees. The controller may inquire about the amount of fees at any given time. The processor will not exercise the right to charge fees unless notifying the controller in advance.

12. Security measures

The processor must implement the following security measures:

Ensure the highest levels of security and data protection in accordance with ISO 27001, GDPR, and PCI-DSS.

Store all data in tier 3+ data centres in Europe that are ISO 27001 certified, secure by design, and redundant.

Have automatic offsite backups in place.

Have policies for vulnerability and patch management, network access, and risk management.

Encrypt all data in both transit and at rest.

13. What happens to the personal data at the end of processing

When the service ends according to this agreement, the processor agrees to erase, and hand over to the controller if requested by the controller, all personal data covered by this agreement.

When personal data is handed over, all copies of personally identifiable data that can be found in the processor's systems must also be erased. When the data has been erased, the processor must demonstrate so in writing.

14. Data Protection Officer

The processor shall send the controller information about the name and contact information of its Data Protection Officer (DPO).

DPO: Dattaca Labs Iceland ehf.

Contact information for DPO:

Address: Ármúli 13, 108 Reykjavik.

Email: dpo@dattacalabs.com

15. Records of processing activities

The processor must keep a record of all processing activities carried out on behalf of the controller. It must state the following:

- the name and contact information of one or more processors, and of any controller for whom the processor acts on behalf of and, as the case may be, the representative of the controller or processor and the DPO,
- categories of processing carried out on behalf of each controller,
- if applicable, transfer of personal data to a third country or international organization, including which third country or international organization is involved, and, in the case of communication referred to in the second subparagraph of Art. 49 (1) GDPR, data on appropriate safeguards,
- if possible, a general description of the technical and organizational security measures referred to in Art. 32 (1) GDPR.

16. Documentation for proof of compliance

The processor must provide the controller with all the necessary documents so that he demonstrate compliance and for the controller or auditor to carry out audits, including inspections, and provide assistance in such audits.

This assistance grants the processor the right to charge fees. The controller may inquire about the amount of fees at any given time. The processor will not exercise the right to charge fees unless notifying the controller in advance.

VIII. Obligations of the controller

The controller shall:

1. deliver the data mentioned in section II to the processor.
2. record in writing all instructions regarding the processing addressed to the processor.

3. ensure, before and during processing, that he works in accordance with the requirements made to him according to the GDPR, and
4. supervise the processing, including by carrying out audits and inspections at the processor.

Annex 1) Overview of data processing activities to be performed by the Processor

1. Controller

The Controller transfers Personal Data identified in the below sections 3, 4 and 5 to the Processor and for the purpose of the processing operations identified in section 6 set out processing activities.

2. Processor

The Processor receives Personal Data identified in the below sections 3, 4 and 5 and processes it in accordance with the processing operations identified in section 6 set out processing activities.

3. Personal data

The Personal Data transferred concerns the following:

a) Token

A random string stored in the CookieHub cookie in the users browser along with the settings for the cookie categories. In case you need to demonstrate the consent, you'll have to request this token from the subject to find the entry from the consent log.

b) Url

The full url that the user was viewing when he configured consents using the CookieHub widget.

c) Anonymized IP address

The IP address of the client. The last part of the IP address is replaced with 0 as IP address could be considered personal information.

d) Country

The registered country code for the IP address. When using geolocation this can be useful to identify if the user consented or didn't get any choices.

e) User agent

The user agent usually contains the browser and operating string information.

f) Date and time

The date and time of consent.

4. Categories of Personal Data

The Categories of Personal Data transferred concerns the following:

a) IP address, Browser information;

b) Country, date and time

c) Indirect Identification Data

5. Special Category Data

The Special Categories of Data transferred concerns the following:

a) None

6. Processing operations

The Personal Data transferred will be subject to the following basic processing activities:

- a)** Personal Data will be processed to the extent necessary to provide the Services in accordance with both the terms of the Agreement and the Controller's instructions. The Processor processes Personal Data only on behalf of the Controller. Processing operations include, but are not limited to the provision of the Services – this operation relates to all aspects of Personal Data processed.

Technical support, issue diagnosis and error correction to ensure the efficient and proper running of the systems and to identify, analyse and resolve technical issues both generally in the provision of the Services and specifically in answer to a Controller query. This operation may relate to all aspects of Personal Data processed but will be limited to metadata where possible.

Annex 2) Approved Sub-processors

| Name | Processing | Country |
|--------------------------|--|-------------------------|
| Amazon Web Services Inc. | Cloud hosting, data storage, monitoring and security solutions | Germany, United Kingdom |
| Online S.A.S. | Cloud hosting, data storage | France, Netherlands |
| UpCloud Ltd | Cloud hosting, data storage | Netherlands |
| Amazon Web Services Inc. | Content delivery network | Worldwide |
| BunnyWay d.o.o. | Content delivery network | Worldwide |
| proinity LLC | Content delivery network | Worldwide |
| Cloudflare | Content delivery network, WAF and DDOS protection | Worldwide |
| Help Scout PBC | Customer support | United States |