January 2023

Privacy Hub DPA
Agreement on data protection for commissioned processing pursuant to Art. 28 DSGVO

Preamble

This DPA is concluded between you (“customer” or “principal”) and Cookiebox GmbH (“service provider” or “contractor”) and is part of the GTC.

Within the scope of contracts concluded or to be concluded, the Contractor processes personal data from the Client’s area of responsibility under data protection law within the meaning of Art. 28 of the German Data Protection Regulation (DSGVO). The personal data provided to the Contractor by the Client shall be subject to the provisions of the DSGVO and the other provisions of data protection law (e.g. BDSG).

This agreement sets out the framework conditions for ensuring compliance with the provisions of data protection law.

1. Subject matter and duration of the order

The subject of the data handling contract is the performance of the following tasks by the contractor: Privacy Hub – an editorial system for the central organisation and implementation of the GDPR requirements on websites, apps and social media accounts. The duration of the contract is indefinite.

2. Concretisation of the content in the contract

Type and purpose of the intended processing of data

More detailed description of the subject matter of the contract with regard to the scope, nature and purpose of the contractor's tasks:

Hosting of the dynamic privacy statement ("Website DSE").

Hosting of the information for data subjects pursuant to Art. 13 / 14 DSGVO ("Data Protection Information DSI)")

The provision of the contractually agreed data processing shall take place exclusively in a member state of the European Union or in another contracting state of the Agreement on the European Economic Area. Any relocation to a third country requires the prior consent of the client and may only take place if the special requirements of Art. 44 et seq. DSGVO are fulfilled.

Type of data

The following types/categories of data are the subject of the processing of personal data (enumeration/description of the data categories)

- Planning and control data
- IP addresses

Categories of data subjects

The categories of data subjects affected by the processing include:

- Website visitors
- Customers
- Prospective customers
- Suppliers
- Sales representatives
- Contact persons

3. Technical and organisational measures

The contractor shall document the implementation of the technical and organisational measures set out and required in the run-up to the awarding of the contract before the start of the processing, in particular with regard to the specific execution of the contract, and shall hand them over to the principal for inspection. If accepted by the Client, the documented measures shall become the basis of the contract. Insofar as the examination/audit of the Client reveals a need for adaptation, this shall be implemented by mutual agreement.

The contractor shall establish security in accordance with Art. 28 Para. 3 lit. c, 32 DSGVO, in particular in connection with Art. 5 Para. 1, Para. 2 DSGVO. Overall, the measures to be taken are data security measures and to ensure a level of protection appropriate to the risk with regard to confidentiality, integrity, availability and the resilience of the systems. In this context, the state of the art, the implementation costs and the nature, scope and purposes of the processing as well as the varying likelihood and severity of the risk to the rights and freedoms of natural persons within the meaning of Article 32 (1) of the GDPR shall be taken into account [details in Annex 1].

The technical and organisational measures are subject to technical progress and further development. In this respect, the contractor is permitted to implement alternative adequate measures. In doing so, the security level of the specified measures must not be undercut. Significant changes shall be documented.

4. Correction, restriction and deletion of data

The contractor may not correct, delete or restrict the processing of data processed under the contract on his own authority but only in accordance with the documented instructions of the principal. Insofar as a data subject contacts the Contractor directly in this regard, the Contractor shall forward this request to the Client without delay.

Insofar as included in the scope of services, the deletion concept, the right to be forgotten, correction, data portability and information shall be ensured directly by the contractor in accordance with the client's documented instructions.

5. Quality assurance and other obligations of the contractor

In addition to compliance with the provisions of this contract, the contractor has legal obligations pursuant to Art. 28 to 33 of the GDPR; in this respect, the contractor shall in particular ensure compliance with the following requirements:

1. The Contractor is not obliged to appoint a data protection officer. Ms Martina Brinkmann is appointed as contact person at the contractor; for contact details see: https://www.cookiebox.pro/datenschutzerklaerung/
2. The maintenance of confidentiality in accordance with Art. 28 Para. 3 Sentence 2 lit. b, 29, 32 Para. 4 DSGVO. When carrying out the work, the contractor shall only use employees who are bound to confidentiality and who have previously been familiarised with the data protection provisions relevant to them. The Contractor and any person subordinate to the Contractor who has access to personal data may process this data exclusively in accordance with the Client's instructions, including the powers granted in this contract, unless they are legally obliged to process it.

3. The implementation of and compliance with all technical and organisational measures required for this contract pursuant to Artt. 28 para. 3 p. 2 lit. c, 32 DSGVO [details in Annex 1].
4. The Principal and the Contractor shall cooperate with the supervisory authority in the performance of their duties upon request.
5. The immediate information of the principal about control actions and measures of the supervisory authority, insofar as they relate to this order. This shall also apply insofar as a competent authority investigates in the context of administrative offence or criminal proceedings with regard to the processing of personal data during the commissioned processing at the Contractor.
6. Insofar as the Client is itself subject to an inspection by the supervisory authority, administrative offence or criminal proceedings, the liability claim of a data subject or a third party or another claim in connection with the commissioned processing at the Contractor, the Contractor shall support it to the best of its ability.
7. The contractor shall regularly monitor the internal processes as well as the technical and organisational measures to ensure that the processing in its area of responsibility is carried out in accordance with the requirements of the applicable data protection law and that the protection of the rights of the data subject is ensured.
8. Verifiability of the technical and organisational measures taken vis-à-vis the Client within the scope of its supervisory powers pursuant to Section 7 of this contract.

6. Subcontracting relationships

Subcontracting relationships within the meaning of this provision are those services which relate directly to the provision of the main service. This does not include ancillary services which the contractor uses e.g. as telecommunication services, postal/transport services, maintenance and user service or the disposal of data carriers as well as other measures to ensure the confidentiality, availability, integrity and resilience of the hardware and software of data processing systems. However, the contractor is obliged to implement appropriate and legally compliant contractual agreements as well as control measures to ensure data protection and data security of the client's data also in the case of outsourced ancillary services.

The list of current sub-service providers can be obtained from the contractor; to do so, simply send an e-mail to post@cookiebox.pro. With the booking of the service, the approval of the sub-service providers is deemed to have been granted. If the client does not agree to the transfer of data to a particular sub-service provider for good cause, both parties may exercise their special right of termination.

The transfer of personal data of the Principal to the subcontractor and its initial activity shall only be permitted once all requirements for subcontracting have been met.

If the subcontractor provides the agreed service outside the EU / EEA, the contractor shall ensure the permissibility under data protection law by taking appropriate measures. The same shall apply if service providers within the meaning of para. 1 sentence 2 are to be used.

Further outsourcing by the subcontractor is generally permitted; all contractual regulations in the contractual chain must also be imposed on the further subcontractor.

7. Control rights of the client

The Client has the right to carry out inspections in consultation with the Contractor or to have inspections carried out by inspectors to be named in individual cases. He has the right to convince himself of the contractor's compliance with this agreement in his business operations by means of spot checks, which as a rule must be notified in good time.

The Contractor shall ensure that the Client can satisfy itself of the Contractor's compliance with its obligations pursuant to Article 28 of the GDPR. The Contractor undertakes to provide the Client with the necessary information upon request and, in particular, to provide evidence of the implementation of the technical and organisational measures.

The proof of such measures, which do not only concern the specific order, can be provided through

- compliance with approved rules of conduct pursuant to Art. 40 DSGVO;
- certification in accordance with an approved certification procedure pursuant to Art. 42 GDPR;
- current attestations, reports or report extracts from independent bodies (e.g. auditors, auditing, data protection officers, IT security department, data protection auditors, quality auditors);
- a suitable certification by IT security or data protection audit (e.g. according to BSI-Grundschutz).

The Contractor may claim remuneration for enabling controls by the Client.

8. Notifications of violations by the contractor

The Contractor shall support the Client in complying with the obligations set out in Articles 32 to 36 of the GDPR regarding the security of personal data, notification obligations in the event of data breaches, data protection impact assessments and prior consultations. These include, but are not limited to.

1. Ensuring an adequate level of protection through technical and organisational measures that take into account the circumstances and purposes of the processing, as well as the predicted likelihood and severity of a potential security breach, and allow for immediate detection of relevant breach events;
2. the obligation to report personal data breaches to the Principal without undue delay;
3. the obligation to support the Principal in its duty to inform the Data Subject and to provide him with all relevant information without undue delay in this context;
4. the support of the Principal for its data protection impact assessment; and
5. supporting the client in the context of prior consultations with the supervisory authority.

The Contractor may claim remuneration for support services which are not included in the service description or which are not due to misconduct on the part of the Contractor.

9. Authority of the principal to issue instructions

The Principal shall confirm verbal instructions without delay (at least in text form).

The Contractor shall inform the Client without delay if he is of the opinion that an instruction violates data protection regulations. The Contractor shall be entitled to suspend the implementation of the corresponding instruction until it is confirmed or amended by the Client.

10. Deletion of data and return of data carriers

Copies or duplicates of the data shall not be made without the knowledge of the Principal. Exceptions to this are backup copies, insofar as they are necessary to ensure proper data processing, as well as data that is required with regard to compliance with statutory retention obligations.

Upon completion of the contractually agreed work or earlier upon request by the Client – at the latest upon termination of the service agreement – the Contractor shall hand over to the Client all documents that have come into its possession, processing and utilisation results produced as well as data files that are related to the contractual relationship or, after prior consent, destroy them in accordance with data protection requirements. The same shall apply to test and reject material. The record of the deletion shall be submitted upon request.

Documentation which serves as proof of orderly and proper data processing shall be kept by the contractor beyond the end of the contract in accordance with the respective retention periods. He may hand them over to the Client at the end of the contract in order to discharge himself.

11. Term and Termination

This agreement shall enter into force upon conclusion of the contract and shall remain valid for as long as the service relationship in question continues.

Annex 1:

I. Technical and organisational measures of the Contractor
II. Technical and organisational measures of the Subcontractor

I. Technical and organisational measures of the contractor

1. Confidentiality (Art. 32 Para. 1 lit. b DSGVO)

- Access control / No unauthorised access to data processing systems
    - Key
- Access control / No unauthorised system use
    - (secure) passwords
    - automatic locking mechanisms
- Access control / no unauthorised reading, copying, modification or removal within the system
    - Authorisation concepts and needs-based access rights
    - Logging of accesses
- Separation control / separate processing of data collected for different purposes
    - Multi-client capability
    - Sandboxing
- Pseudonymisation (Art. 32 Abs. 1 lit. a DSGVO; Art. 25 Abs. 1 DSGVO) / The processing of personal data in such a way that the data can no longer be attributed to a specific data subject without the use of additional information, provided that this additional information is kept separately and is subject to appropriate technical and organisational measures.

2. Integrity (Art. 32 Abs. 1 lit. b DSGVO)

- Disclosure control - No unauthorised reading, copying, modification or removal during electronic transmission or transport
    - encryption
- Determination of whether and by whom personal data have been entered into, altered or removed from data processing systems.
    - Logging

3. Availability and resilience (Art. 32 Abs. 1 lit. b DSGVO)

- Availability control - Protection against accidental or deliberate destruction or loss
  - Backup strategy (online/offline; on-site/off-site)
  - Virus protection
  - Firewall
- rapid recoverability (Art. 32 Abs. 1 lit. c DSGVO);

4. Procedures for regular review, assessment and evaluation (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)

- Data protection management
- Incident-Response-Management
- Data protection-friendly default settings (Art. 25 para. 2 DSGVO)
- Commissioning control - No commissioned data processing within the meaning of Art. 28 DSGVO without corresponding instructions from the client
  - Clear contract design
  - Formalised order management
  - Strict selection of the service provider
  - Obligation to convince in advance
  - Follow-up checks

II. Technical-organisational measures of the sub-service provider

V1.0 from 01.01.2023

Preamble

The sub-service provider leases the data processing system to the client. This includes the leasing of hardware and software, as well as the provision of connections to the Internet and other services in accordance with the respective agreement. The Principal alone and exclusively decides which personal data are processed in which manner. The data processing programmes required for this purpose shall be created and used by the Principal. The sub-service provider shall ensure the technical operational readiness of the system in accordance with the contractual agreements and shall keep records of which systems are used by the Principal and to what extent. Data processing shall be carried out by the Principal. The subcontractor has no influence whatsoever on the data processing operations carried out by the principal.

Confidentiality (Art. 32 Abs. 1 lit. b DSGVO)

Access control

No unauthorised access to data processing equipment in the data processing centres.

1. access control system
A locking system in the form of at least 1-factor authentication (e.g. transponder, chip card, bell system with personal control by image and sound) allows access to data processing facilities only after a positive access check.

2. key control
The issuing of keys to persons for access to data processing facilities is documented.

3. logging of visitors
Visitors who gain access to data processing systems (e.g. in the event of hardware replacement by the manufacturer) are recorded in a visitor book.

4. intrusion alarm system
Access to data processing facilities is protected by an intrusion alarm system.

5. video surveillance
Data processing facilities are secured by video surveillance.

Access control

No unauthorised system use

1. password assignment
In principle, access to data processing systems is only possible by means of a combination of a user name and the assigned password.

2. password policy
Passwords for data processing systems must meet minimum complexity requirements of the company-wide policy; employee passwords must be changed regularly.

3. administrative access
All data processing systems shall be accessible for maintenance purposes exclusively via approved IP address ranges and in encrypted form (e.g. VPN restrictions).

4. firewall
Protection of the infrastructure by firewalls (software and/or hardware), restrictions of unused ports as well as user name and password against unauthorised access. Systems providing

main contract services will be equipped with a firewall according to the respective agreement in the main contract.

5. use of anti-virus software
Systems used to access data processing systems are equipped with anti-virus software. This software is regularly updated to the latest virus definitions. Systems providing customer services will be equipped with anti-virus software as agreed in the main contract.

6. encryption of mobile data carriers
If mobile data carriers or mobile devices are used, the contents shall be encrypted.

Access control

No unauthorised reading, copying, modification or removal within the system.

1. allocation of user rights
Access to data processing systems is restricted for persons to the minimum necessary data in each case by assigning appropriate user rights. The data processing itself is carried out by the customer The contractor has no influence whatsoever on the data processing operations carried out by the customer.

2. Secure storage of data carriers
Data carriers containing personal data shall be stored in a locked location.

3. administration of rights by a restricted group of persons
Only authorised system administrators are able to manage the rights of other persons to data processing systems. The circle of authorised system administrators is reduced to the smallest possible selection of persons. The data processing itself is carried out by the client. The contractor has no influence whatsoever on the data processing operations carried out by the client.

4. logging of accesses
Accesses to services (e.g. web services) are logged in log files in compliance with the DSGVO. The data processing itself is carried out by the customer. However, the contractor has no influence whatsoever on the data processing operations carried out by the customer.

5. proper destruction of data carriers
Data carriers containing personal data shall be destroyed in accordance with DIN 66399.

6. regular maintenance of data processing systems

Separation control

Separate processing of data collected for different purposes

1. definition of database rights
Access to databases by systems and users is restricted to the data required in each case.

2. separation of productive and test systems
Production and test environments are operated in isolation from each other. Access by one environment to data in the other environment is prevented by the use of e.g. separate database systems and server systems.

3. logical client separation
Separation of data from clients is ensured by the use of different software mechanisms.

Integrity (Art. 32 Abs. 1 lit. b DSGVO)

1. disclosure control
No unauthorised reading, copying, alteration or removal during electronic transmission or transport.

2. Transport
If personal data is passed on, this is always done in encrypted form. The data processing itself is carried out by the client. The contractor has no influence whatsoever on the data processing operations carried out by the client.

3. input control
Determining whether and by whom personal data have been entered into, changed or removed from data processing systems.

4. assignment of rights
Access to data processing systems shall be restricted for persons to the minimum necessary data in each case by assigning appropriate user rights.

5. logging of data entries
Data processing shall be carried out by the customer. The contractor shall have no influence on the data processing programmes used by the customer. The input control of the data can therefore only be implemented by the customer.

6. traceability of the input
The data processing is carried out by the customer. The contractor has no influence on the data processing programmes used by the client. The input control can therefore only be

implemented by the customer. In the event of changes by the contractor, the administration accesses shall be adequately logged.

Availability and resilience (Art. 32 Abs. 1 lit. b DSGVO)

Availability control

Protection against accidental or deliberate destruction or loss

1. uninterruptible power supply in server rooms (data centres)
Server rooms are protected by uninterruptible power supplies. The protection is two-tiered. If necessary, an emergency power unit is automatically activated to take over the power supply of the server rooms.

2. air-conditioning systems in server rooms (data centres)
An appropriate temperature and humidity for the operation of server systems is ensured in server rooms by adequately dimensioned air-conditioning systems.

3. fire and smoke detection systems in server rooms (data centres)
Fire and smoke detection systems are used to detect fires at an early stage. Fire extinguishing systems extinguish any fires that occur.

4. data backup concept and storage of data backups
Data backups of personal data shall only be made by agreement or in accordance with the main contract concluded and shall be stored on separate systems dedicated to data backups.

5. Monitoring
System-critical instances are monitored. The data processing itself is carried out by the customer. The Contractor has no influence whatsoever on the data processing operations carried out by the Client.

Procedures for regular review, assessment and evaluation (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)

Data protection management

The contractor shall establish a data protection management system that ensures the protection of personal data.

Incident-Response-Management

Regular review of the IT infrastructure. The contractor shall establish an incident response plan.

Data protection-friendly default settings (Art. 25 Abs. 2 DSGVO)

The contractor shall ensure within its possibilities that only data that are absolutely necessary for the respective specific processing purpose are processed by means of default settings. The data processing itself is carried out by the customer. The contractor has no influence whatsoever on the data processing operations carried out by the client.

Order control

No commissioned processing within the meaning of Art. 28 DSGVO without corresponding instructions from the client.

1. selection of suitable contractors
When selecting contractors who process personal data on behalf of the client, only contractors who at least comply with the legally prescribed requirements for the processing of personal data shall be selected.

2. monitoring of contractors
The contractor is regularly checked for compliance with the assured technical and organisational measures for the processing of personal data.