

Storyblok GmbH
Peter-Behrens-Platz 2
4020 Linz, Österreich
ATU72706128



Agreement

on

Data processing to Art. 28 GDPR

Person responsible:

Processor:

Storyblok GmbH
Peter-Behrens-Platz 2
4020 Linz, Österreich

(hereinafter referred to as the data controller)

(hereinafter referred to as the data processor)

1. OBJECT OF THE AGREEMENT

- (1) The object of this order is the data processing in connection with the Storyblok platform. Storyblok provides a cloud-based web application for content maintenance. The application enables end consumers to store their own content to be used with electronic media on the data controller's platforms and to save it for later use with an e-mail and password. This agreement serves as a supplement to the general Terms and Conditions "Terms" (<https://www.storyblok.com/terms>), "Acceptable Use Policy (AUP)" (<https://www.storyblok.com/acceptable-use-policy/>) and to the "Privacy Policy" <https://www.storyblok.com/privacy-policy>).
- (2) The following data will be processed:
- a. Contact details
 - b. Communication data
 - c. Billing details
 - d. Address details
 - e. Analysis data

- f. Order and billing details
 - g. Contractual details
- (3) The following categories of people shall be subject to the processing:
- a. Clients of the Storyblok platform
 - b. License holders
 - c. Suppliers
 - d. Employees
 - e. Interested parties
 - f. Website visitors

2. DURATION OF THE AGREEMENT

The agreement is unlimited in time and can be terminated by both parties. The possibility of extraordinary termination for cause or in the case of a breach of the "Terms" (<https://www.storyblok.com/terms>) by the data controller remains unaffected.

3. DUTIES OF THE DATA PROCESSOR

- (1) The data processor undertakes to process data and processing results exclusively pursuant to the data controller's written orders. If the data processor receives an official order to disclose the data of the data controller, they are obliged to - if legally allowed - inform the data controller immediately and refer the official authority to them. Also, data processing for the data processor's own purposes requires a written order.
- (2) In a legally binding manner, the data processor declares that all the contracted persons had been obliged to maintain confidentiality or that they are subject to an appropriate legal duty of confidentiality prior to taking up their activity. In particular, the duty of confidentiality shall remain in force for the persons involved in the data processing also after their employment and services for the data controller have ceased.
- (3) In a legally binding manner, the data processor declares to have taken all necessary measures to guarantee the security of data processing in accordance with Art 32 GDPR (details to be found in Appendix ./1).
- (4) The data processor shall take the technical and organisational measures to enable to data controller to fulfil the rights of the person concerned pursuant to Chapter III of the GDPR (information, disclosure, correction and deletion, data portability, objection, as well as automated decision making in individual cases) within the statutory deadlines at any time and shall provide the data controller with all the necessary information. If a request is submitted to the data processor and they indicate to have been mistakenly considered the processor of the data operated, the data processor shall immediately forward the request to the data controller and inform the requesting body accordingly.
- (5) The data processor shall assist the data controller in complying with the obligations within the Articles 32 to 36 of the GDPR (data security measures, reports to supervisory authorities concerning

violation to the personal data protection, notification of the person affected by a violation to the personal data protection, data protection impact assessment, prior consultation).

- (6) The data processor shall be informed about the obligation to establish and update a processing list according to Art 30 GDPR for the present order processing.
- (7) The data controller or a third-party contracted by them, shall be granted the right to inspect and control the data processing systems at any time. The data processor undertakes to provide the data controller with the information necessary to review the compliance with the obligations determined in this agreement.
- (8) After termination of this agreement, the data processor is obliged to forward all the processing results and documents containing data to the data controller or to remove them on their behalf. If the data processor processes the data in a specific technical format, they are obliged, after termination of this agreement, to provide the data either in the same format or at the request of the data controller in a format, in which they had received the data from the data controller or in a different common format.
- (9) The data processor shall immediately inform the data controller if they consider an instruction from the data controller as violating the data protection regulations of the EU or the Member States.

4. PLACE OF THE DATA PROCESSING

Data processing activities are also carried out, at least in part, outside the EU or the EEA, in the United States. The adequate level of data protection results from:

- an adequacy decision of the European Commission under Article 45 GDPR.
- Standard data protection clauses in accordance with Article 46 (2) (c) and (d) GDPR.

5. SUB-PROCESSOR

The data processor is allowed to consult the following companies as sub-processors:

Sub-processor	Country	Service
Amazon Web Services	United States	Hosting Provider
Stripe Payment Europe	Ireland	Payment Provider
Crisp	France	Chat Provider
Hubspot	United States	CRM Provider
Google	Ireland	Storage Provider
Mailchimp	United States	Mail Provider

Twilio	United States	Messaging Provider
Auth0	United States	SSO Provider

The data processor is to inform the data controller about their intention to consult a sub-process in a timely manner, so that the data controller has enough time to prohibit it. The data processor shall conclude the required agreements pursuant to Art. 28, para. 4 GDPR with the sub-processor. It shall be ensured that the sub-processor assumes the same obligations pursuant to this agreement as the data processor. Should the sub-processor fail to comply with their data protection obligations, the data processor shall be liable to the data controller for sub-processor's compliance with the obligations.

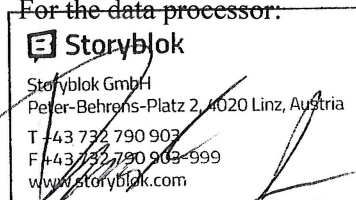
_____, _____

Linz, 23.05.2018

For the data controller:

.....
[]

For the data processor:



.....
[CEO, Eng. Dominik Angerer]

Appendix ./1 - technical and organisational measures

CONFIDENTIALITY

- **Access control:** Access control against unauthorised entrance to the data processing systems, e.g.: Key, swipe or chip cards, electric door openers, porters, security personnel, alarm systems, video systems; the internal data processing systems are only accessible to the administrator with a key and possible with a two-step authentication.
- **Access control:** Protection against unauthorised system use thorough passwords (including appropriate policy), automatic locking mechanisms, two-step authentication, encryption of data carriers; all computers and accesses are protected through passwords. There are defined employees with the access to the Cloud Services infrastructure. These are tied to the authentication system of our Amazon accounts and secured through a two-step authentication. Upon leaving the company, the user's account along with the further access possibilities deactivated.
- **Access control:** No unauthorised reading, copying, changing or deleting possible. Access to the database is secured with a password and two-step authentication. Access to the server is only possible via SSH and for authorised users. Both are only accessible via internal network (a password-protected VPN if needed). Granted authorisations are periodically reviewed. All accesses/log-ins of the internal system shall be registered.
- **Pseudonymisation:** If possible for the respective data processing, the primary identification features of the personal data shall be removed within the respective data application and stored separately.
- **Data classification scheme:** Due to the statutory obligations or self-assessment (confidential/classified/internal/public).

INTEGRITY

- **Disclosure control:** No unauthorised reading, copying, changing or deleting during electronic forwarding or transport, e.g.: Encryption, Virtual private Networks (VPN), electronic signature;
- **Input control:** Review concerning if and who entered, changed or deleted personal data into and from the data processing system. Automatic logging of the accesses and changes.

AVAILABILITY AND CAPACITY

- **Availability control:** Protection against random or deliberate destruction or loss, e.g.: Backup strategy (on-line/off-line; on-site/off-site), uninterrupted power supply (UPS, diesel generator), virus protection, firewall, reporting channels and emergency plans; security checks at the infrastructure and application level, multi-level security concept with encrypted outsourcing to a backup data centre, standard processes in case of staff transfer/retirement;
- **Rapid recoverability;**
- **Deletion periods:** For the data as well as the meta data such as log files, etc.

PROCEDURES FOR REGULAR REVIEW, ASSESSMENT AND EVALUATION

- Data protection management: Systemic security tests are conducted at irregular intervals by a third-party data processor. The results are recorded.
- The incident-response-management is conducted and reported.
- Default privacy settings of our users: All new profiles are set to private by default.
- Order control: No processing of order data pursuant to Art 28 GDPR without corresponding instructions from the data controller, e.g.: transparent contract design, formalised order management, strict selection of the order processor (ISO certification, ISMS), due diligence, follow-up controls.