

Data Processing Addendum

Frontify AG, Version: Mai 2019

between

Company Name

Street

City

Country

hereinafter referred to as "Customer" or "Party"

and

Frontify AG

Unterstrasse 4

9000 St. Gallen

Switzerland

hereinafter referred to as "Frontify" or "Party"
or together with Customer as "Parties"



1. Introduction

This Data Processing Addendum to Frontify Customer Agreement (as defined below) including its appendices (the “**DPA**”) reflects the Parties’ agreement with respect to the terms governing the processing and security of Customer Data under the applicable agreement. The DPA will, as from the Addendum Effective Date (as defined below), be effective and replace any terms previously applicable to privacy, data processing and/or data security.

2. Definitions

In this DPA, unless stated otherwise:

“**Affiliate**” means any entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity. “Control”, for purposes of this definition, means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity.

“**Addendum Effective Date**” means: (a) if this DPA is incorporated into the applicable Frontify Customer Agreement by reference, the Effective Date of that Frontify Customer Agreement; or (b) otherwise, means the date on which Customer clicked to accept or signed this DPA or the Parties otherwise agreed to this DPA.

“**Controller**” means the entity which determines the purposes and means of the Processing of Personal Data.

“**Controller Affiliate**” means any of Customer's Affiliate(s) (a) that are subject to applicable Data Protection Laws of the European Union, the European Economic Area and/or their member states, Switzerland and/or the United Kingdom, and permitted to use the Services pursuant to the Frontify Customer Agreement, but have not signed their own order form and are not a “Customer” as defined under the Agreement, (b) if and to the extent Frontify Processes Personal Data for which such Affiliate(s) qualify as the Controller.

“**Customer**” for the purposes of this DPA only, and except where indicated otherwise, the term “Customer” shall include Customer and Customer Affiliates.

“**Customer Data**” means data submitted, stored, sent or received via the Services by Customer, its Affiliates or End Users.



“Customer Personal Data” means Personal Data contained within the Customer Data.

“Data Protection Laws” means all laws and regulations, including laws and binding regulations of the European Union, the European Economic Area and their member states, Switzerland and the United Kingdom, applicable to the Processing of Personal Data under the Agreement.

“Data Subject” means the identified or identifiable natural person to whom Personal Data relates.

“End User” means all individual natural person which uses the Services (e.g. employees of Customer).

“European Data Protection Legislation” means, as applicable: (a) the GDPR; and/or (b) the Federal Data Protection Act of 19 June 1992 (Switzerland).

“Frontify” means Frontify AG or Frontify Deutschland GmbH, as applicable based on which of the Frontify legal entities signed the Frontify Customer Agreement with the Customer.

“Frontify Customer Agreement” means either (a) Master Services Agreement signed between Customer and Frontify; or (b) one or more Order Form(s) specifying that Frontify will provide the Services to the Customer; or (c) any other agreement under which Frontify agrees to provide the Services to the Customer.

“GDPR” means the General Data Protection Regulation (EU) 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.

“Personal Data” means any Customer Data that relates to an identified or identifiable natural person, to the extent that such information is protected as personal data under applicable Data Protection Laws.

“Processing” means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

“Processor” means the entity which Processes Personal Data on behalf of the Controller.

“Services” means products and services as defined in the applicable Frontify Customer Agreement.



“Standard Contractual Clauses” means the clauses adopted by European Commission Decision 2010/87/EU on February 5th 2010.

“Sub-Processor” means any entity engaged by Frontify to Process Personal Data in connection with the Services.

“Supervisory authority” means an independent public authority which is established by a member state pursuant to Article 51 of the GDPR.

“Term” means the period from the Amendment Effective Date until the end of Frontify’s provision of the Services under the applicable Frontify Customer Agreement, including, if applicable, any period during which provision of the Services may be suspended and any post-termination period during which Frontify may continue providing the Services for transitional purposes.

Other capitalized terms used but not defined in this DPA have the meanings given elsewhere in the applicable Frontify Customer Agreement.

3. General Terms

This DPA forms a part of the Frontify Customer Agreement. In case the Frontify Customer Agreement was signed before this DPA was established, Frontify may engage with the Customer to execute this DPA separately.

If the Customer is not a party to a Frontify Customer Agreement, this DPA is not valid and is not legally binding. In this case the Customer should request that the Customer entity who is a party to the applicable Frontify Customer Agreement executes this DPA.

By signing the DPA, Customer enters into this DPA on behalf of itself and, to the extent required under applicable Data Protection Laws, in the name and on behalf of its Controller Affiliates.

In the course of providing the Services under the Frontify Customer Agreement, Frontify may Process certain Personal Data (such terms defined below) on behalf of Customer and where Frontify Processes such Personal Data on behalf of Customer the Parties agree to comply with the terms and conditions in this DPA in connection with such Personal Data.



3.1. How to Execute this DPA

This DPA consists of two parts: the main body of the DPA and Exhibit A. The DPA has been pre-signed on behalf of Frontify. To complete this DPA, Customer must:

1. complete the notification information in section 12;
2. complete the information in the signature box in section 14 and
3. send the completed and signed DPA to Frontify by email via privacy@frontify.com.

Upon receipt of the validly completed DPA by Frontify at this email address, this DPA will become legally binding.

4. Processing of Data

4.1. Roles and Regulatory Compliance; Authorization

4.1.1 Processor and Controller Responsibilities

If the European Data Protection Legislation applies to the Processing of Customer Personal Data, the Parties acknowledge and agree that:

- a) the subject matter and details of the Processing are described in Exhibit A;
- b) Frontify is a Processor of that Customer Personal Data under the European Data Protection Legislation;
- c) Customer is a Controller or Processor, as applicable, of that Customer Personal Data under the European Data Protection Legislation; and
- d) each Party will comply with the obligations applicable to it under the European Data Protection Legislation with respect to the Processing of that Customer Personal Data.

4.1.2 Authorization by Third-Party Controller

If the European Data Protection Legislation applies to the Processing of Customer Personal Data and Customer is a Processor, Customer warrants to Frontify that Customer's instructions and actions with respect to that Customer Personal Data, including its appointment of Frontify as another Processor, have been authorized by the relevant Controller.



4.1.3 Responsibilities under Non-European Legislation

If Non-European Data Protection Legislation applies to either Party's Processing of Customer Personal Data, the Parties acknowledge and agree that the relevant Party will comply with any obligations applicable to it under that legislation with respect to the Processing of that Customer Personal Data.

4.2. SCOPE OF PROCESSING

4.2.1 Customer's Instructions

By entering into this DPA, Customer instructs Frontify to Process Customer Personal Data only in accordance with applicable law: (a) to provide the Services and related technical support; (b) as further specified via Customer's use of the Services and related technical support; (c) as documented in the form of the applicable Frontify Customer Agreement, including this DPA; and (d) as further documented in any other written instructions given by Customer and acknowledged by Frontify as constituting instructions for purposes of this DPA.

4.2.2 Legality of Processing

Customer shall, in its use of the Services and provision of instructions, use and Process Customer Personal Data in accordance with the requirements of applicable Data Protection Laws. Customer shall have sole responsibility for the accuracy, quality, and legality of Customer Personal Data and the means by which Customer acquired Customer Personal Data.

4.2.3 Frontify's Compliance with Instructions

As from the Addendum Effective Date, Frontify will comply with the instructions described in Section 4.2.1 (Customer's Instructions) (including with regard to data transfers) unless EU or EU Member State law to which Frontify is subject requires other Processing of Customer Personal Data by Frontify, in which case Frontify will inform Customer (unless that law prohibits Frontify from doing so on important grounds of public interest) via the Notification Email Address. For clarity, Frontify will not Process Customer Personal Data for advertising purposes or serve advertising in the Services.

4.3. Return and Deletion of Personal Data

Frontify will enable Customer and/or End Users to delete Customer Data during the applicable Term in a manner consistent with the functionality of the Services. If Customer or an End User uses the Services to delete any Customer Data during the applicable Term and the Customer Data cannot be recovered by Customer or an End User (such as recovery from the "trash" within 30 days after deletion), this use will constitute an instruction to Frontify to delete the relevant Customer Data from Frontify's systems in accordance with applicable law. Frontify will comply with this instruction as



soon as reasonably practicable and within a maximum period of 180 days, unless EU or EU Member State law or Swiss law requires storage.

Upon termination of the Services for which Frontify is Processing Customer Personal Data, Frontify shall, upon Customer's request, and subject to the limitations described in the Frontify Customer Agreement return all Personal Data in Frontify's possession to Customer or securely destroy such Personal Data and demonstrate to the satisfaction of Customer that it has taken such measures, unless applicable law prevents it from returning or destroying all or part of Personal Data. For clarification, depending on the Service plan purchased by Customer, access to export functionality may incur additional charge(s) and/or require purchase of a Service upgrade.

Frontify may retain Customer Data that is (i) contained in an archived computer system back-up in accordance with security and/or disaster recovery procedures; (ii) contained in latent data, including deleted files and other non-logical data types such as memory dumps, swap files, temporary files, printer spool files and metadata that are not generally retrievable or accessible without the use of specialized tools and techniques; (iii) prepared for regulatory compliance, archival or record retention purposes; or (iv) retained by legal counsel only for purposes of confirming compliance with this DPA, subject in each case to the destruction of such Customer Data in due course and the inaccessibility of such Customer Data to Frontify and its representatives in the ordinary course of business, and further that in each case such Customer Data shall remain subject to the terms and conditions of this DPA.

5. Rights of Data Subject

Data Subject Rights; Data Export. During the applicable Term, Frontify will, in a manner consistent with the functionality of the Services, enable Customer to access, rectify and restrict Processing of Customer Data, including via the deletion functionality provided by Frontify as described in Section 4.3, and to export Customer Data.

Customer's Responsibility for Data Subject Requests. During the applicable Term, if Frontify receives any request from a Data Subject in relation to Customer Personal Data, Frontify will advise the Data Subject to submit his/her request to Customer, and Customer will be responsible for responding to any such request including, where necessary, by using the functionality of the Services.

Frontify's Data Subject Request Assistance. Customer agrees that (taking into account the nature of the Processing of Customer Personal Data) Frontify will assist Customer in fulfilling any obligation to



respond to requests by Data Subjects, including if applicable Customer's obligation to respond to requests for exercising the Data Subject's rights laid down in Chapter III of the GDPR.

6. Sub-Processors

6.1. Sub-Processor Engagement

Customer specifically authorizes the engagement of Frontify's Affiliates as Sub-Processors. In addition, Customer generally authorizes the engagement of other third-parties as Sub-Processors. When engaging a Sub-Processor, Frontify will:

- a) ensure via a contract (written and/or electronic form) that:
 - 1. the Sub-Processor only accesses and uses Customer Data to the extent required to perform the obligations subcontracted to it, and does so in accordance with the applicable Frontify Customer Agreement (including this DPA); and
 - 2. if the GDPR applies to the Processing of Customer Personal Data, the data protection obligations set out in Article 28(3) of the GDPR, as described in this DPA, are imposed on the Sub-Processor.
- b) remain fully liable for all obligations subcontracted to, and all acts and omissions of, the Sub-Processor.

6.2. Information about Current Sub-Processors

A current list of Sub-Processors for the Services, including the identities of those Sub-Processors and their country of location is attached as Exhibit B ("**Sub-Processor List**").

6.3. Opportunity to Object to Sub-Processor changes

When any new Sub-Processor is engaged during the applicable Term, Frontify will, at least 30 days before the new Sub-Processor processes any Customer Personal Data, inform Customer of the engagement (including the name and location of the relevant Sub-Processor and the activities it will perform) either by sending an email to the Notification Email Address or via the admin console.



Customer may object to any new Sub-Processor (e.g., if making Personal Data available to the Sub-Processor may violate applicable Data Protection Law or weaken the protections for such Personal Data) by notifying Frontify promptly in writing within 10 business days after receipt of Frontify's notice. Such notification must be sent to privacy@frontify.com and contain a description of a reasonable ground for the objection.

Frontify will use commercially reasonable effort to analyze any valid concerns raised by the Customer in respect to the new Sub-Processor and mitigate the reported issues (including a potential replacement of the Sub-Processor if any critical issues were raised).

If no agreement was achieved, Customer may terminate the applicable Frontify Customer Agreement immediately upon written notice to Frontify, on condition that Customer provides such notice within 90 days of being informed of the engagement of the Sub-Processor.

Frontify will refund Customer any prepaid fees covering the remainder of the term of the applicable Frontify Customer Agreement following the effective date of termination with respect to such terminated Services, without imposing a penalty for such termination on Customer.

6.4. Liability of Sub-Processors

Frontify shall be liable for the acts and omissions of its Sub-Processors to the same extent Frontify would be liable if performing the Services of each Sub-Processor directly under the terms of this DPA.

7. Security

7.1. Controls for the Protection of Personal Data

Frontify shall maintain appropriate technical and organizational measures for protection of the security (including protection against unauthorized or unlawful Processing and against accidental or unlawful destruction, loss or alteration or damage, unauthorized disclosure of, or access to, Personal Data), confidentiality and integrity of Personal Data. Customer can request the Data Security Policy via emailing privacy@frontify.com with the subject "Data Security Measures". Thereafter, Frontify will provide Customer its Data Security Policy.



7.2. Audits

Upon Customer's request, and subject to the confidentiality obligations set forth in the Frontify Customer Agreement, Frontify shall make available to Customer (or Customer's independent, third-party auditor) information regarding Frontify's compliance with the obligations set forth in this DPA. Customer may contact Frontify in accordance with the contact information as defined in the Frontify Customer Agreement to request an on-site audit of Frontify's procedures relevant to the protection of Customer Personal Data, but only to the extent required under applicable Data Protection Law. Customer shall reimburse Frontify for any time expended for any such on-site audit at Frontify's then-current rates, which shall be made available to Customer upon request. Before the commencement of any such on-site audit, Customer and Frontify shall mutually agree upon the scope, timing, and duration of the audit, in addition to the reimbursement rate for which Customer shall be responsible. All reimbursement rates shall be reasonable, taking into account the resources expended by Frontify. Customer shall promptly notify Frontify with information regarding any non-compliance discovered during the course of an audit, and Frontify shall use commercially reasonable efforts to address any confirmed non-compliance.

7.3. Confidentiality

Frontify shall ensure that its employees, contractors, and agents who are authorized to Process Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

8. Personal Data Incident Management and Notification

Frontify maintains security incident management policies and procedures specified in the Data Security Policy. Frontify shall notify Customer without undue delay of any breach relating to Customer Personal Data (within the meaning of applicable Data Protection Law) of which Frontify becomes aware and which may require a notification to be made to a Supervisory Authority or Data Subject under applicable Data Protection Law or which Frontify is required to notify to Customer under applicable Data Protection Law ("**Personal Data Incident**"). Frontify shall provide commercially reasonable cooperation and assistance in identifying the cause of such Personal Data Incident and take commercially reasonable steps to remediate the cause to the extent the remediation is within Frontify's control. Except as required by applicable Data Protection Law, the obligations herein shall not apply to incidents that are caused by Customer, End Users and/or any Non-Frontify Products.



9. Limitation of Liability

Each Party's and all of its Affiliates' liability, taken together in the aggregate, arising out of or related to this DPA, and all DPAs between Controller Affiliates and Frontify, whether in contract, tort or under any other theory of liability, is subject to the Limitation of Liability section of the Frontify Customer Agreement, and any reference in such section to the liability of a Party means the aggregate liability of that Party and all of its Affiliates under the Frontify Customer Agreement and all DPAs together.

For the avoidance of doubt, Frontify's and its Affiliates' total liability for all claims from the Customer and all of its Controller Affiliates arising out of or related to the Frontify Customer Agreement and each DPA shall apply in the aggregate for all claims under both the Frontify Customer Agreement and all DPAs established under the Frontify Customer Agreement, including by Customer and all Controller Affiliates, and, in particular, shall not be understood to apply individually and severally to Customer and/or to any Controller Affiliate that is a contractual party to any such DPA.

10. European Specific Provisions

10.1. GDPR

Applicability. With effect from 25 May 2018, Frontify is Processing Personal Data in accordance with the GDPR requirements where applicable to Frontify's provisioning of the Services.

Data Protection Impact Assessment. Upon Customer's request, Frontify shall provide Customer with reasonable cooperation and assistance needed to fulfil Customer's obligation under the GDPR to carry out a data protection impact assessment related to Customer's use of the Services, to the extent Customer does not otherwise have access to the relevant information, and to the extent such information is available to Frontify. Frontify shall provide reasonable assistance to Customer in the cooperation or prior consultation with the Supervisory Authority, to the extent required under the GDPR.

10.2. Transfer Mechanisms

As of the effective date of this DPA, Frontify only works with Sub-Processors of the United States which signed the Standard Contractual Clauses and/or self-certify to and comply with the EU-U.S.



and Swiss-U.S. Privacy Shield Frameworks (whichever is applicable), as administered by the US Department of Commerce.

11. Applicable Law and Place of Jurisdiction

This DPA and any dispute or claim arising out of or in connection with it or its subject matter or formation (including non-contractual disputes or claims) shall be governed by, and construed in accordance with, the laws of Switzerland.

In the event of any differences of opinion in connection with this DPA or its Exhibits, the Parties undertake to attempt to agree to a mutually agreed regulation in good faith. If, despite the efforts of the Parties, no agreement can be made by amicable means, the place of jurisdiction for all disputes, differences of opinion or claims arising from or in connection with the contractual relationship between Frontify and the Customer including their validity, invalidity, violation or dissolution, shall be St. Gallen, Switzerland.

12. Notification

Customer agrees that Frontify will use the following contact details for any notifications related to this DPA:

Name (written out in full): _____
Position: _____
Email: _____

13. Final Provisions

13.1. Written Form and Amendments to this DPA

This DPA, its Exhibits, any amendments and supplements, as well all side agreements, shall be set out in writing and signed by both Parties in order to be valid. These formal requirements may only



be waived by means of a written agreement. This also applies in particular to this written form clause. No amendment to this DPA will be effective unless it is agreed to in writing by both Parties.

13.2. Severability Clause

Should individual provisions of this DPA be invalid or incomplete or should performance be impossible, this shall not negatively affect the validity of the remaining provisions of this DPA. Invalid provisions shall be replaced by an admissible, valid provision that is as close as possible to the content of the original in terms of its intent.

13.3. Counterparts and Electronic Signature

This DPA may be executed using electronic or digital signatures, which shall have the same force and effect as a manual signature. This DPA may also be signed in counterparts, each of which shall be deemed an original, and all of which together shall constitute one and the same contract.



14. Signatures

The Customer

Place, date

Name, signature

Place, date

Name, signature

Frontify AG

Place, date

Name, signature

Place, date

Name, signature

List of Exhibits

Exhibit A: Subject Matter and Details of Processing Activities

Exhibit B: Sub-Processor List



Exhibit A

Subject Matter and Details of Processing Activities

Subject matter. Frontify's provision of Services and related technical support to Customer.

Duration of the Processing. The applicable Term plus the period from expiry of such Term until deletion of all Customer Data by Frontify in accordance with this DPA.

Nature and Purpose of the Processing. Frontify will Process Customer Personal Data submitted, stored, sent or received by Customer, its Affiliates or End Users via the Services for the purposes of providing the Services and related technical support to Customer in accordance with this DPA.

Categories of Data. Personal Data submitted, stored, sent or received by Customer, its Affiliates or End Users via the Services may include the following categories of data: user IDs, email, documents, graphical material (e.g. photos and images), and other data.

Data Subjects. Personal Data submitted, stored, sent or received via the Services may concern the following categories of Data Subjects: End Users including Customer's employees and contractors; the personnel of Customer's customers, suppliers and subcontractors; and any third-parties that Customer conducts business with and provides access to Services.



Exhibit B

Sub-Processor List

Sub-Processor	Location	Service of Sub-Processor
Amazon Web Services (AWS)	Frankfurt DE or North Virginia USA <i>(depending on the Frontify Customer Agreement)</i>	Data processing and hosting
Wildbit (Postmark)	Philadelphia USA	Email processing
Algolia	Paris FR	Real-time search
Pusher	London UK	Real-time messaging
Intercom	San Francisco USA	In-App Support/ Chat-System