Frontify

Data processing agreement

Frontify AG, version: March 2026
Pick date

between

Legal name
Street
City
Country

hereinafter referred to as “Customer” or “Party”

and

Frontify AG
Unterstrasse 4
9000 St. Gallen
Schweiz

hereinafter referred to as “Frontify” or “Party”
and together with Customer as the “Parties”

privacy@
frontify.com

Frontify

Table of contents

Frontify

Frontify

1. Preamble

In the course of providing the Frontify Services under the Agreement between Frontify and Customer, Frontify may Process Personal Data on behalf of Customer. The Parties agree to comply with the terms of this Data Processing Agreement including its appendices (altogether referred to as **"DPA"**), which are incorporated into and form part of the Agreement. In case of any conflict between the terms of this DPA and other terms of the Agreement, the terms of this DPA will govern.

The Parties acknowledge and agree that Customer may qualify as a Controller or Processor in relation to Personal Data of its personnel, providers, customers, and/or other third parties involved by Customer (**"Customer Personal Data"**). As a result:

- where Customer is a Controller, Frontify shall be a Processor; and
- where Customer is a Processor, Frontify shall be a Sub-Processor.

This DPA reflects the Parties' commitment to abide by Data Protection Laws with respect to the Processing of Customer Personal Data under the terms of the Agreement. The categories of Personal Data and Data Subjects Processed under this DPA, as well as the subject matter, duration, and nature of the Processing, are further specified in Exhibit A (Subject Matter and Details of Processing Activities).

2. Definitions

Unless otherwise defined in this DPA or the Agreement, all terms listed in this section shall have the meaning indicated herein.

"**Effective Date**" means the effective date of the Agreement.

"**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, or otherwise having the power to govern the financial and the operating policies or to appoint the management of the subject entity.

"**Agreement"** means the Frontify License Agreement, Order form, or other written or electronic agreement concluded between Frontify and Customer for the use of the Frontify Services, including all its attachments, in particular, but not limited to, the

Offer, the GTC, the Service Level Agreement and any other additional document governing the contractual relationship between the Parties.

"AI Features" means artificial intelligence or machine learning functionalities that Frontify may offer within the Frontify Platform to streamline asset management and support brand consistency.

"Controller" means the entity which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.

"**Customer**" shall include, for the purposes of this DPA only, and except if indicated otherwise, a customer of Frontify under the Agreement, including such customer's Affiliates.

"**Customer Data**" means all data, including Customer Personal Data, submitted, stored, sent, or received via the Frontify Services by Customer, its Affiliates, or Platform Users.

"Customer Notification Email Address" means the email address which is specified in the Agreement as the Customer contact for legal and/or privacy notifications; or, if no email address is specified in the Agreement, the email address of one or more Customer contacts on Frontify's record.

"**Data Protection Laws**" means all laws and regulations applicable to the Processing of Personal Data under the Agreement and which may include but are not limited to the GDPR, the laws of the EEA and its member states, Switzerland, the United States of America, and the United Kingdom.

"**Data Subject**" means the individual to whom Personal Data relates.

"**Data Subject Request**" is a demand made by a Data Subject who seeks to exercise its Data Subject's right to access, rectify, erase, transfer, or port Customer Personal Data or to restrict or object to the Processing of Customer Personal Data in accordance with Chapter III GDPR.

"**EEA**" means the European Economic Area.

"**Frontify**" means Frontify AG.

"Frontify Notification Email Address" means privacy@frontify.com.

"Frontify Platform" means the software supplied by Frontify to Customer for use via the Internet, namely the all-in-one web-based brand management SaaS solution, the mobile app, and the desktop app offered by Frontify.

"**Frontify Services**" means the services offered by Frontify and purchased by Customer under the Agreement, both currently and in the future, including the subscription to the Frontify Platform.

"**GDPR**" means the Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27 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).

"**Personal Data**" means any information that directly or indirectly identifies a Data Subject under the Data Protection Laws.

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

"Processor" means a natural or legal person, public authority, agency or other body which Processes Personal Data on behalf of the Controller.

"Adequate Jurisdiction" means (i) where the GDPR applies, a country for which the European Commission has issued an adequacy decision within the meaning of art 45(1), (ii) where the UK GDPR applies, a country for which an adequacy decision has been issued pursuant to Section 17A of the Data Protection Act 2018, and (iii) where the Swiss DPA applies, a country which is listed in Annex 1 of the Federal Data Protection Ordinance (SR 235.11).

"Standard Contractual Clauses" or "SCC" means Commission Implementing Decision (EU) 2021/914 of June 4, 2021, on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council.

"**Sub-Processor**" means any third party engaged by Frontify to provide services necessary to perform the Frontify Services, and that will participate in the Processing of Customer Personal Data.

"Swiss Data Protection Law" means the Federal Act on Data Protection (SR 235.1) and the Federal Data Protection Ordinance (SR 235.11).

"Technical and Organizational Measures" or **"TOMs"** means a set of rules, guidelines, policies, and procedures designed to ensure that all users, servers, networks, and

processes within an organization fulfil the adequate level of security and data protection standards required under Data Protection Laws.

“Term” means the period starting from the Effective Date until the cessation of the provision of the Frontify Services under the Agreement. This includes, if applicable, any period during which the provision of the Frontify Services may be suspended and any period following the termination of the Agreement during which Frontify may continue providing the Frontify Services for transitional purposes.

“Third-Party Products and Services” means independent third-party products and services not licensed directly by Frontify, including but not limited to web-based, mobile, offline, or other software functionalities that interoperate with the Frontify Services. Third-Party Products and Services may be provided by Customer or a third-party and enabled at Customer’s option to extend the experience and functionality of the Frontify Services.

“UK Data Protection Law” means the Data Protection Act 2018 and the United Kingdom General Data Protection Regulation.

“Platform User” means any natural person who is authorized to use the Frontify Platform under the Agreement.

Frontify

3. Execution & duration

3.1. Introduction

This DPA is an integral part of the Agreement and does not need to be executed separately. Either Party enters this DPA on behalf of itself and, to the extent required and/or permitted under Data Protection Laws, in the name and on behalf of its Affiliates.

This DPA shall, as from the Effective Date, become legally binding and replace any terms previously agreed by the parties regarding privacy, data processing, and/or data security. This DPA shall terminate automatically upon termination of the Agreement or as earlier terminated pursuant to the terms set forth herein.

3.2. Parts of this DPA

This DPA consists of four (4) parts:

- The main body of the DPA;
- Exhibit A (Subject matter and details of Processing activities);
- Exhibit B (Sub-Processor list);
- Exhibit C (Technical and organizational measures)

4. Roles and regulatory compliance

4.1. Controller and Processor

In full compliance with their respective roles and responsibilities under the Data Protection Laws, Customer in its quality as Controller or Processor, and Frontify in its quality as Processor or Sub-Processor, acknowledge and agree that:

a) the subject matter and details of the Processing are described in Exhibit A;
b) each Party will comply with the obligations of the Data Protection Laws with respect to the Processing of Customer Personal Data.

4.2. Authorization by third-party Controller

As far as Customer is a Processor, Customer warrants that Customer's instructions and actions concerning Customer Personal Data, including the appointment of Frontify as a Sub-Processor, have been duly authorized by the relevant Controller.

Frontify

5. Processing

5.1. Scope of Processing

By entering this DPA, the Parties agree that Frontify will only Process Customer Personal Data in connection with the provision of the Frontify Services and/or on Customer's documented instructions.

The subject matter and details of Processing are specified in Exhibit A and Frontify will solely rely on those, unless further Processing is (a) required by applicable laws, (b) based on Customer's documented instructions, or (c) otherwise agreed by the Parties in writing. If and to the extent applicable laws require further Processing of Customer Personal Data, Frontify will, as far as legally permitted, promptly inform Customer by email at the Customer Notification Email Address.

Frontify shall notify Customer if it believes that Customer's documented instructions violate Data Protection Laws and shall be entitled to suspend the execution of the relevant instruction until Customer provides an instruction that complies with Data Protection Laws. If Customer's documented instructions violate Data Protection Laws, Customer shall indemnify and hold Frontify harmless against all claims, damages and liabilities arising from such instructions.

5.2. Legality of Processing

Customer shall, in its use of the Frontify Services and provision of instructions, Process Customer Personal Data in accordance with the requirements of the Data Protection Laws, including but not limited to the obligation to inform the Data Subjects of the use of Frontify as Processor. Customer shall be solely responsible for the accuracy, quality, and legality of Customer Personal Data and the manner in which the Customer Personal Data is collected.

5.3. Deletion or return of Customer Personal Data

During the Term, Frontify will enable Customer and/or Platform Users to delete Customer Data through the functionalities of the Frontify Services. If Customer or a Platform User deletes any Customer Data, this will be removed from the Frontify' systems in accordance with applicable law.

Following the termination of the Agreement, and upon written request, Frontify will provide Customer with a copy of the Customer Data on a customary data carrier or by electronic transfer in a format agreed to by the Parties. Ninety (90) days after the effective date of termination of the Agreement or, at Customer's request, even earlier, Frontify will delete all Customer Data from its systems, except where legal retention requirements prevent Frontify from doing so.

Frontify

Frontify may retain Customer Data that is (a) contained in an archived computer system back-up in accordance with security and/or disaster recovery procedures; (b) 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; (c) prepared for regulatory compliance, archival or record retention purposes in accordance with applicable law; or (d) 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 by Frontify and its personnel in the ordinary course of business. In each case such Customer Data shall remain subject to the terms and conditions of the DPA.

Customer Personal Data stored in the system backups will be automatically deleted three hundred sixty-five (365) days after the creation of the backup. Upon written request, Frontify shall provide Customer with a statement certifying that Customer Personal Data has been destroyed.

6. Sub-Processing

6.1. Engagement of Sub-Processors

Customer generally agrees that Frontify may use Sub-Processors to fulfil its contractual obligations under the Agreement. Therefore, Customer authorizes the engagement of Frontify's Affiliates and of third parties as Sub-Processors, to the extent the conditions set forth in this section 6 and in section 10 are complied with.

Frontify will enter into a written agreement with each Sub-Processor including data protection obligations that are substantially equivalent to those agreed in this DPA, considering the nature, scope, context and purposes of the services provided by the Sub-Processor.

Frontify warrants that the Sub-Processor shall access and Process Customer Data only to the extent necessary to perform the obligations subcontracted to it in accordance with the Agreement, including this DPA.

Frontify shall be liable for all obligations subcontracted to the Sub-Processors and for all acts and omissions of the Sub-Processors to the same extent as Frontify would be liable if Frontify directly provided the services of each Sub-Processor in accordance with the terms of this DPA. All limitations of liability set out in the Agreement or this DPA shall apply equally to the acts and omissions of Sub-Processors.

6.2. List of Sub-Processors and involvement of new Sub-Processors

Frontify's current Sub-Processors are listed in Exhibit B (**"Sub-Processor List"**). When a new Sub-Processor is engaged, Frontify shall update the Sub-Processor List and notify Customer at the Customer Notification Email Address at least fourteen (14) days prior to giving the new Sub-Processor access to Customer Personal Data.

Customer may object to any new Sub-Processor on reasonable and legitimate grounds (e.g., if the involvement of the new Sub-Processor may violate Data Protection Laws), by giving written notice at the Frontify Notification Email Address within fourteen (14) days of the relevant communication. Customer's written objection shall outline the Customer's specific concerns about the new Sub-Processor in order to give Frontify the opportunity to address such concerns. Frontify shall use commercially reasonable efforts to analyze any valid concerns and may, at its sole discretion: (a) decide to not appoint the new Sub-Processor and/or propose an alternative Sub-Processor; (b) take steps to remedy or mitigate Customer's specific concerns and obtain Customer's written consent to use the new Sub-Processor; or (c) make available to Customer the Frontify Services without the service or functionality provided by the new Sub-Processor. If Frontify is unable or reasonably determines, that it is commercially unreasonable to do any of the above options, Customer may extraordinarily terminate the affected parts of the Frontify Services by giving written notice within thirty (30) days. Frontify shall refund to Customer the pro-rata amount of any prepaid fees for the remainder of the Term following the effective date of termination with respect to such terminated Frontify Services, without imposing a penalty for such termination on Customer.

7. Rights of Data Subjects

During the Term, Frontify will enable Customer to access, rectify, restrict, delete, and export Customer Personal Data through the functionalities of the Frontify Services.

In the event any Data Subject Request is made directly to Frontify in connection with Frontify's Processing of Customer Personal Data, Frontify will, to the extent legally permitted, promptly notify Customer and provide details of the same, or will advise the Data Subject to submit the request directly to Customer. Customer will be responsible for responding to a Data Subject Request, including, where necessary, by using the functionalities of the Frontify Services.

Frontify will assist the Customer in fulfilling its obligations under Data Protection Laws, including the obligation to respond to requests from Data Subjects.

Frontify

8. Security

8.1. Technical and organizational measures ("TOMs")

Frontify shall comply with the obligations imposed by the Data Protection Laws regarding the security of Customer Personal Data. More specifically, Frontify shall, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of the Processing of Customer Personal Data as well as the risk of varying likelihood and severity for the rights and freedoms of Data Subjects, implement and maintain appropriate technical and organizational measures to ensure a level of security appropriate to the risk in accordance with Art. 32 GDPR. The TOMs form an integral part of the DPA and are attached as Exhibit C.

The TOMs may change or be replaced from time to time. However, Frontify shall ensure that no such change or replacement will ever diminish the appropriate level of security for Customer Personal Data.

8.2. Audit and reports

Upon Customer's written request and subject to confidentiality obligations, Frontify shall provide Customer (or Customer's independent third-party auditor) with information regarding Frontify's compliance with the obligations set forth in the DPA. Frontify shall engage external auditors to verify the adequacy of its security measures. Such audits shall (a) be performed at least annually in the light of the ISO 27001 standards or any alternative standards that are substantially equivalent to ISO 27001; (b) be performed by independent third-party security professionals at Frontify's selection and expense; and (c) result in the generation of an audit report ("Report"), which shall be considered Frontify's confidential information. Upon Customer's written request, Frontify shall provide a copy of the Report.

If, despite the foregoing, Customer intends to perform an additional audit on Frontify's procedures affecting Customer Personal Data, Customer shall submit a request to Frontify and Frontify agrees to it provided that a) such audit is required under Data Protection Laws, and b) a similar audit has not been already conducted less than twelve (12) months prior. However, the above restrictions shall never hinder the performance of such supplementary audit, where there have been indications of data protection violations and/or the audit is requested by a supervisory authority or other competent regulatory authority. The Customer shall reimburse Frontify for the time invested in the audit at Frontify's current rates, which will be made available to Customer upon request. Before the commencement of such audit, the Parties shall mutually agree upon its scope, timing, and duration, as well as the reimbursement rate for which Customer shall be responsible. All reimbursement rates shall be reasonable, considering the resources invested by Frontify. Customer shall promptly notify Frontify of any non-compliance discovered during an audit, and Frontify shall use

commercially reasonable efforts to resolve any non-compliance acknowledged by Frontify. The parties agree to keep the information related to such audit strictly confidential.

8.3. Confidentiality and training

Frontify shall ensure that its employees and contractors who are authorized to Process Customer Data are bound by confidentiality obligations and Frontify shall organize periodic employee training sessions on privacy, confidentiality, and data security.

8.4. Incident management and notification

Frontify shall maintain security incident management policies and procedures. Frontify shall notify the Customer without undue delay and in any event within forty-eight (48) hours of becoming aware of any breach relating to Customer Personal Data that may require notification to a supervisory authority, Data Subject or Customer under Data Protection Laws (**"Data Breach"**). The notification of a Data Breach will be delivered by email at the Customer Notification Email Address and shall indicate at least the following:

- the nature of the Data Breach including, where possible, the categories and approximate number of Data Subjects concerned and the categories and approximate number of Personal Data records concerned;
- the name and contact details of the data protection officer or other contact point where more information can be obtained;
- the likely consequences of the Data Breach;
- the measures taken or proposed to be taken by Frontify to address the Data Breach, including, where appropriate, measures to mitigate its possible adverse effects.

In the event that it is not possible to provide the above information at the same time as the notification, this will be provided in later stages without undue delay.

The Parties agree that Frontify's notification of a Data Breach shall never be considered an acknowledgement by Frontify of any fault or liability in that regard. Frontify shall, to the extent commercially reasonable cooperate to identify the cause of such Data Breach and, where the remediation is within Frontify's control, take all reasonable steps to remediate such cause without delay. Except as required by Data Protection Laws, the obligations herein shall not apply to incidents that are caused by Customer, Platform Users, or any Third-Party Products and Services.

Frontify

9. AI Features and data processing

In connection with the provision of the AI Features through the Frontify Platform, Frontify shall maintain all necessary technical and organizational measures to ensure a responsible, secure, and compliant Processing in accordance with Data Protection Laws and this DPA.
Frontify represents that, as of the Effective Date, the AI Features operate without requiring any Processing. However, the Parties acknowledge that incidental Processing may occur where Customer includes Personal Data in prompts, instructions, or guidelines submitted to the AI Features; where Personal Data is contained in the output generated by the AI Feature; or where Personal Data forms part of other Customer Data uploaded to or otherwise made available through the Platform (collectively "Content Data").
To the extent Personal Data is Processed in connection with the AI Features, Frontify shall: i) Process such Personal Data solely for the purpose of providing AI Features to Customer in accordance with the Agreement and the Customer's documented instructions; ii) not Process Personal Data for any other purpose, including for training, developing, improving, or fine-tuning artificial intelligence or machine learning models, except where such Processing is performed exclusively for the benefit of the Customer and does not result in the Personal Data being used to improve models for other customers or general use; or as otherwise expressly authorised by Customer in writing.
To provide the AI Features, Frontify may engage third-party technology providers acting as Sub-Processors. In that case, Frontify shall ensure that: i) such providers are subject to documented privacy and security due diligence prior to engagement; ii) a written data processing agreement is executed with each Sub-Processor that contains obligations substantially equal to those of this DPA; iii) Sub-Processors are contractually prohibited from using Customer Data for their own purposes, including for model training, development, or improvement; and iv) appropriate security, confidentiality, and incident response obligations are contractually imposed.

The third-party AI providers currently engaged by Frontify in connection with the AI Features are listed in Exhibit B. Any such providers shall be treated as Sub-Processors under this DPA.
Frontify may introduce new AI Features from time to time. Where such an introduction results in material changes to the Processing of Personal Data or the engagement of new Sub-Processors, Frontify shall update this DPA and/or the applicable Sub-Processor list in accordance with the provisions set forth herein for all Sub-Processors.

Frontify

10. Limitation of liability

Each Party's and its Affiliates' liability, taken together in the aggregate, arising out of, or related to this DPA, whether in contract, tort, or under any other theory of liability, is subject to the limitation of liability set forth in the Agreement.

11. Hosting location and data transfers

11.1. Hosting location

Depending on the Customer's selection in the Agreement, Customer Personal Data will be hosted on data servers located in the EEA or the USA. Additionally, Customer Personal Data will be Processed at Frontify's headquarter in Switzerland. A transfer of Customer Personal Data to a country outside an Adequate Jurisdiction shall take place only if it complies with Data Protection Laws and to the extent the conditions set forth in this section 10 are met.

11.2. Data transfers under the GDPR

With regard to Processing activities that involve a transfer of Customer Personal Data to a location outside an Adequate Jurisdiction, the Parties hereby agree that Frontify shall ensure compliance with Chapter V GDPR by adopting the measures required under art. 46(2) GDPR. Such measures may include, without limitation, transferring Customer Personal Data (a) to a Sub-Processor that has achieved binding corporate rules authorization in accordance with art 47 GDPR; or (b) to a Sub-Processor that has executed the Standard Contractual Clauses. The applicable data transfer mechanism for each Sub-Processor is specified in the Sub-Processor List (Exhibit B).

In the event that a decision of the European Commission authorizing the transfer of Personal Data outside the EEA is invalidated or a supervisory authority requires the suspension of the transfer of Personal Data, Frontify will implement an alternative data transfer mechanism that will allow Customer to continue to benefit from the Frontify Services in compliance with Data Protection Laws.

11.3. Data transfer under UK Data Protection Laws

To the extent that UK Data Protection Law applies to Customer Personal Data and insofar as required under UK Data Protection Law, Frontify will only transfer Personal Data to a location outside an Adequate Jurisdiction if the measures required under the UK Data Protection Law and the instructions of the Information Commissioner of the UK have been implemented.

11.4. Data transfer under Swiss Data Protection Laws

To the extent that Swiss Data Protection Law is applies to Customer Personal Data and insofar as required under Swiss Data Protection Law, Frontify will only transfer Personal Data to a location outside an Adequate Jurisdiction if the measures required under the Swiss Data Protection Law and the instructions of the Swiss Federal Data Protection and Information Commissioner have been implemented.

12. Customer assistance and governmental inquiries

Upon request and to the extent required under Data Protection Laws, Frontify shall, taking into account the information available to it and provided that Customer does not otherwise have access to the same, reasonably assist Customer in performing its relevant obligations under Art. 32 to 36 GDPR.

If Frontify is compelled to disclose Customer Personal Data to law enforcement or other governmental authorities, Frontify will, to the extent permitted by law, provide Customer with reasonable notice to enable Customer to seek appropriate remedies against such disclosure orders.

To the extent legally permitted, Customer shall reimburse Frontify for the time invested in Customer assistance at Frontify's current rates, which shall be made available to Customer upon request.

13. Final provisions

13.1. Severability clause

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

13.2. Amendments to this DPA

Frontify may amend this DPA from time to time and will provide prior written notice of any material amendments.
The Customer may object to a material amendment on reasonable grounds by providing written notice within fifteen (15) days of receipt of such notice. The Parties shall discuss the objection in good faith. If the Parties are unable to resolve a valid objection within a reasonable period, the previous version of the DPA shall remain in

effect; provided, however, that any amendments required by applicable data protection laws shall take effect as required by such laws. If the Customer does not object within the above-mentioned period, the updated version of the DPA shall be deemed accepted.

13.3. Applicable law and place of jurisdiction

This DPA and any dispute or claim arising out of or in connection with it (including non-contractual disputes or claims) shall be governed by, and construed in accordance with the governing law and dispute resolution provisions set forth in the Agreement.

If the Agreement does not specify the governing law or jurisdiction, this DPA shall be governed by the laws of Switzerland, excluding conflict of laws principles, and subject to the exclusive jurisdiction of the courts of St.Gallen, Switzerland.

Frontify

14. Signatures

Customer

Place, date	Name, title	Signature
Place, date	Name, title	Signature

Frontify AG

Place, date	Name, title	Signature
Place, date	Name, title	Signature

List of exhibits

Exhibit A: Subject matter and details of Processing activities
Exhibit B: Sub-Processor list
Exhibit C: Technical and organizational measures (TOMs)

Frontify

Exhibit A - Subject matter and details of Processing

Subject matter. The subject matter is the provision of the Frontify Services and related support to Customer.

Duration of the Processing. The Processing activities will be performed during the Term, as well as during the period between the expiry of the Term and the deletion of Customer Personal Data by Frontify in accordance with the DPA.

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

Categories of Personal Data. Frontify Processes the following categories of Personal Data in connection with the Frontify Services:

1. Mandatory Platform User Information required for login purposes:

- Name
- Email address

2. Optional Platform User Information voluntarily provided by Users:

- Profile picture
- Job title
- Company name

3. Information regarding the Platform User's usage of the Frontify Platform ("Platform Usage Data"):

- IP address
- geographical location inferred from IP address (regional level)
- browser type and version
- referral source
- language preference
- length of visits
- conversation data with support

- interactions with functionalities of the Frontify Platform (e.g., pages viewed, download and upload history)

This information may be collected for the following purposes: i) Frontify Platform operation, maintenance and security, ii) improving the Frontify Platform quality, design, and performance, iii) notifying Platform Users of new features, services, trainings, help articles, tailored reports, webinars, and other events, and iv) inviting Platform Users to participate in product research surveys to improve their experience using the Platform.

Frontify processes Platform Usage Data generally in pseudonymized or aggregated form. In specific cases, Frontify will de-pseudonymize an individual Platform User for any of the above purposes and only selected Frontify employees have access to de-pseudonymized Platform Usage Data if necessary to complete a required task.

4. Information processed in connection with the Customer Hub services (including mandatory Platform User information listed above, as well as the following additional categories):

- Scheduling & Calendar Information
- Company name
- Frontify user role
- Unique User IDs
- Legal contact
- Billing contact

5. Information embedded in assets ad/or processed in connection with the use of AI features:

- Content Data

The uploading of Content Data is exclusively managed by the Customer and the Platform Users and falls outside the direct control of Frontify. The Customer and Platform Users are responsible and liable for the usage of the Content Data and the lawfulness of the Processing.

Categories of Data Subjects. Customer independently determines which individual shall be granted access to the Frontify Platform. Typically, Platform Users can be classified according to the following categories of Data Subjects:

- Customer's employees
- Customer's contractors (e.g. external consultants)

Frontify

Exhibit B - Sub-Processor list

Third-party-provider

Provider	Legal name of provider	Address	Service description	Data retention	Location of Data Processing	Categories of Personal Data	Categories of Data Subjects	Special categories of Personal Data	Data transfer mechanism
ActiveCampaign (Postmark)	AC PM, LLC	1 N Dearborn Street, Suite 500, Chicago, IL 60602, USA	Transactional email service	45 days	USA	email address / IP address / geographical location inferred from IP address (regional level) / opening status	Platform User	No	Adequate Jurisdiction (Provider is certified under the Data Privacy Framework)
Amazon Web Services	Amazon Web Services EMEA SARL	38 Avenue John F. Kennedy, L-1855, Luxembourg, Luxembourg	Cloud service provider and AI services, incl. Amazon Bedrock, Amazon Textract, and Amazon Rekognition to power the AI Features	Data will be stored for the duration of the customer agreement	Germany or USA (depending on the individual agreement between Frontify and the customer)	All data that is necessary to run the Frontify Platform incl. all database data. Content Data for AI services	Platform User	No	Adequate Jurisdiction (Provider is certified under the Data Privacy Framework)
Amplitude	Amplitude Inc.	201 3rd Street, Suite 200, San Francisco, CA 94103, USA	Anonymized product analytics	Data will be anonymized after a logical second since data collection	Germany	IP address / Platform Usage Data (anonymized)	Platform User	No	Adequate Jurisdiction (Provider is certified under the Data Privacy Framework)
Intercom	Intercom R&D Unlimited Company	2nd Floor, Stephen Court, 18-21 St. Stephen's Green, Dublin 2, Ireland	In-app support / User onboarding / Feedback collection / Product updates / Knowledge base	Data will be stored for the duration of the customer agreement	USA	Name / email address / Platform Usage Data	Platform User	No	Adequate Jurisdiction (Provider is certified under the Data Privacy Framework)
Datadog	Datadog Inc.	620 8th Avenue, 45th Floor, New York, NY 10018-1741, USA	Monitoring and observability of the Frontify Platform	30 days	Germany	Email address / IP address / Platform Usage Data	Platform User	No	Adequate Jurisdiction (Provider is certified under the Data Privacy Framework)
Splunk	Splunk LLC	250 Brannan Street, San Francisco, CA 94107, USA	Security Information and Event Management tool (SIEM)	365 days	Germany	Email address / IP address / Platform Usage Data	Platform User	No	Adequate Jurisdiction (Provider is certified under the Data Privacy Framework)
EverAfter	EverAfter AI Ltd	82 Yigal Alon, Tel Aviv, Israel 6789124	Customer Hub operation (incl. onboarding and enablement/ communication and updates/ self-Service support and education/ account	Data will be stored for the duration of the customer agreement	Germany	Name / Email address / Scheduling & Calendar Information / Company name / Frontify User role / Unique User ID) / Legal Contact/ Billing contact	Platform User	No	Adequate Jurisdiction

			management/ automated renewals for Growth and Self-Guided custo mers)						
Microsoft	Microsoft Ireland Operations Limited	One Microsoft Place, South Country Business Park, Leopardstown Dublin 18, D18P521, Ireland	Azure AI services to power the AI Features	30 days	Germany	Content Data	Platform User	No	Adequate Jurisdiction (Provider is certified under the Data Privacy Framework)
Langfuse	Finto Technologies GmbH	Gethsemanestr. 4, 10437, Berlin, Germany	Monitoring and analysis of the AI Features' input and outputs	90 days	Ireland	Content Data	Platform User	No	Adequate Jurisdiction

Frontify

Affiliates

Provider	Legal Name of provider	Address	Service description	Data retention	Location of Data Processing	Categories of Personal Data	Categories of Data Subjects	Special categories of Personal Data	Data transfer mechanism
Frontify Inc.	Frontify Inc.	625 Broadway, Floor 12, New York, NY 10012, USA	Support services	Data will be stored for the duration of the customer agreement	USA	Name / email address / Platform Usage Data	Platform User	No	SCC
Frontify UK Ltd.	Frontify UK Ltd.	5 New Street Square, EC4A 3TW London, UK	Support services	Data will be stored for the duration of the customer agreement	United Kingdom	Name / email address / Platform Usage Data	Platform User	No	Adequate Jurisdiction
Frontify Deutschland GmbH	Frontify Deutschland GmbH	Friedrich-Ebert-Anlage 36, 60325 Frankfurt am Main, Germany	Support services	Data will be stored for the duration of the customer agreement	Germany	Name / email address / Platform Usage Data	Platform User	No	Adequate Jurisdiction
TwicPics SAS	TwicPics SAS	10, rue de Penthievre, 75008 Paris, France	Support services	Data will be stored for the duration of the customer agreement	France	Name / email address / Platform Usage Data	Platform User	No	Adequate Jurisdiction

Frontify

Exhibit C - Technical and organizational measures (TOMs)

Frontify AG, Version: April 2023

1. Preamble

Frontify's information security program is designed in accordance with best practice industry standards, such as ISO 27001. Frontify's security controls are designed to address its posture as a cloud-based software-as-a-service (SaaS) provider. The following concepts apply to Frontify's software and its provision of the services (hereinafter "Frontify Services") and are contextually important to understanding Frontify's security measures.

Frontify has implemented appropriate technical and organizational measures (hereinafter "TOMs") to ensure a level of security appropriate to the risk of the processing activities performed to provide the Frontify Services. The TOMs shall take into account the state of the art, the costs of implementation, the nature, scope, context, and purposes of the processing, as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons.

The TOMs are subject to regular improvement and development; therefore, Frontify may review and update this document from time to time. In this respect, Frontify is entitled to implement adequate alternative measures, which shall not materially diminish the overall security level of the measures specified herein.

As Frontify uses the services of an external hosting partner, both for the hosting and processing of data, some measures will be solely implemented in the data center of such hosting partner. Accordingly, the TOMs which only concern the hosting partner are indicated in this document with the addition ("Hosting-Partner").

2. Audits and certifications

Frontify ensures that a yearly audit of the implemented information security program is performed by an external auditor and, upon request, provides its customers with documentation of proof of compliance by making available industry certificates (e.g., ISO 27001 certification, Cyber Essentials certification) and excerpts of audit results, subject to the condition that such customer is bound to confidentiality obligations.

3. Secure cloud hosting

The Frontify Services are performed using the secure server infrastructure of our cloud hosting partner AWS.

For more information about the security standards implemented by AWS, please refer to:

- https://aws.amazon.com/security/
- https://aws.amazon.com/compliance/programs/
- https://aws.amazon.com/compliance/data-center/controls/

4. Information security policy

Frontify has implemented an information security policy that governs all the relevant aspects of its security program and is aligned with best practice industry standards such as ISO 27001 requirements. Frontify's information security policy may be made available to customers upon request, subject to the condition that the customer is bound to confidentiality obligations. Further information on Frontify's security controls can be accessed at https://www.frontify.com/en/security/.

5. Anonymization and pseudonymization

Anonymization of personal data involves the removal of personal identifiers, the aggregation of data, or the processing of data in such a way that it can no longer be associated with an individual person. Pseudonymization reduces the direct reference to an individual person during the processing in such a way that only the inclusion of additional information allows an assignment to that person.

To the extent technically possible and compatible with the provision of the Frontify Services, Frontify anonymizes personal data. Where anonymization is not possible, Frontify resorts to pseudonymization of personal data. However, in order to provide the Frontify Services, anonymization or pseudonymization of personal data is not always feasible and would be contrary to the purpose of the Frontify Services.

Frontify

6. Encryption

Encryption is a measure or process that allows to convert information into an illegible, (i.e., not easily interpretable) character string (ciphertext), with the aid of an encryption method (cryptosystem).

6.1. Encryption during transmission (data in transit)

The Frontify Services are only available on pages with HTTPS, and HSTS headers are created for all subdomains. Frontify leverages Transport Layer Security (TLS) 1.2 (or better) for data in transit over any network. Frontify supports full data encryption in transit. No non-encrypted data leaves the data center. All monitoring and backend systems either send local traffic over the VPC (virtual private cloud) or use transport-level encryption when communicating with the rest of the Internet.

6.2. Encryption of resting data (data at rest)

Customer data is stored in encrypted form, in S3 buckets, and it is logically separated. Frontify encrypts data at rest using the Advanced Encryption Standard (AES) 256-bit (or better).

7. Confidentiality

Frontify adopts effective measures to ensure the confidentiality of data and to prevent any unauthorized disclosure of or access to transmitted, stored or otherwise processed data. These measures include physical access control, admission control, access control, and separation control.

7.1. Physical access control

Measures to ensure that unauthorized persons are prevented from gaining access to the data processing infrastructure.

Description of the physical access control:

- controlled key management
- door protection (electronic door-opener)
- monitoring system (alarm system)
- control system for visitors
- Hosting-Partner: site security, gatekeeper
- Hosting-Partner: server room protection

7.2. Admission control

Measures to ensure that unauthorized persons are prevented from accessing the data.

Description of the admission control:

- password policy, i.e., personal and individual user log-in when accessing the system (e.g., special characters, minimum length)
- automatic locking (e.g., password, pause mode)
- creation of a user master record per user
- limiting the number of authorized employees
- encryption of data storage
- access lists
- isolation of sensitive systems through separate network areas
- authentication procedure (VPN, certificates, multi-factor authentication)
- logging of login attempts and interruption of the login process after a defined number of unsuccessful attempts

7.3. Access control

Measures to ensure that those authorized to access a data processing infrastructure can only access the data that is subject to their access authorization. This ensures that data cannot be read, copied, modified, or removed without authorization during processing and storage.

Description of the access control:

- concept based on the principle of the least privilege
- authorization concepts (differentiated authorizations in profiles, roles, etc.)
- encryption of different data storage
- logging of accesses and attempted misuse

7.4. Separation control

Measures to ensure that data collected for different purposes are processed separately and kept separate from other data and systems, in order to exclude unplanned use of these data for other purposes.

Description of the separation control:

- authorization concepts (differentiated authorizations in profiles, roles, etc.)
- encrypted storage of data
- multi-tenant environment with logical customer separation
- separation of test and production systems

Frontify

8. Integrity

Measures to maintain integrity of data to prevent data from being modified in an unnoticed, unauthorized, or unintentional manner. These measures include data integrity, transmission control, transport control, and input control.

8.1. Data integrity control

Measures to ensure that data is not damaged or altered by malfunctions of the system.

Description of the data integrity control:

- implementation of new releases and patches with a release/patch management
- operational test during implementation and releases/patches by the IT department
- logging
- transport processes with individual responsibility

8.2. Transmission control

Measures to ensure that it is possible to verify and determine where data has been or can be transmitted or made available using data transmission facilities.

Description of the transmission control:

- logging
- transport processes with individual responsibility
- hashing

8.3. Transport control

Measures to ensure that the confidentiality and integrity of data is protected during the transmission of data and transport of data carriers.

Description of the transport control:

- transmission of data via encrypted data networks or tunnel connections (VPN)
- transport processes with individual responsibility
- encryption procedures which detect data modifications during transport
- comprehensive logging procedures

8.4. Input control

Measures that allow to check and establish whether and by whom the data in the data processing infrastructure have been entered, modified, or removed.

Description of the input control:

- logging of all system activities and retention of these logs for at least one year
- protocol analysis systems
- hashing
- digital signatures

9. Vulnerability detection and management

Frontify uses threat detection tools to ensure that suspicious activities, potential malware, viruses, and/or malicious computer codes are detected and reported to Frontify.

By default, Frontify scans all file types for malware (malware scanning) and uses input validation measures to prevent the execution of programs in files uploaded by the user that contain malware. In addition, Frontify enables its customers to add specific file types to a block list.

Frontify has implemented a bug bounty program to ensure continuous vulnerability detection throughout the year.

Vulnerabilities that meet defined risk criteria trigger automatic alerts and are prioritized for remediation based on their potential threat and impact on the Frontify Services.

10. Data neutrality

Frontify does not review the data uploaded by customers to the Frontify Services and processes all data regardless of its nature provided it fits the predefined characteristics for processing. Frontify makes no data-based decisions, but only executes customers' instructions when they upload content to the Frontify Services to achieve the desired results.

Frontify

11. Administrative controls

Frontify performs criminal background screening on its employees as part of its hiring process, as appropriate given the employee's role and as permitted under applicable law.

Frontify conducts regular training sessions on data privacy and security. Further, every employee is required to complete an onboarding program.

Frontify employees are bound by confidentiality either under their respective employment contracts or under a separate confidentiality agreement.

Frontify employees are bound to the adherence of information security policies either under their respective employment contracts or under a separate statement of acceptance.

12. Availability and resilience

Measures to ensure the availability and resilience of data processing equipment, to ensure that high loads or high continuous loads are feasible and that access to the data is restored in a timely manner in the event of a physical or technical incident. Such measures include availability control, timely recovery of availability, and reliability.

12.1. Availability control

Measures to ensure that data is protected against accidental destruction or loss.

Description of the availability control:

- Hosting-Partner: data backup procedures
- Hosting-Partner: uninterrupted power supply
- Hosting-Partner: fire alarm system
- Hosting-Partner: air conditioning
- Hosting-Partner: alarm system
- Hosting-Partner: emergency plans
- Hosting-Partner: no water-carrying pipes above or next to server rooms

12.2. Timely recovery of availability

Measures to ensure that the availability of and access to data is promptly restored in the event of a physical or technical incident.

Description of the timely recovery of availability:

- data backup procedures
- regular tests of the data recovery
- disaster and emergency plans
- off-site backup
- Hosting-Partner: availability zones

12.3. Reliability

Measures to ensure that all functions of the system are available and that any malfunctions are reported.

Description of the reliability:

- automatic monitoring with e-mail notification
- disaster and emergency plans with responsibilities
- regular tests of the data recovery

13. Security incident reporting

If Frontify becomes aware of a security incident that results in the accidental or unlawful destruction, loss, alteration, disclosure, or access of customer personal data, Frontify will promptly notify affected customers in accordance with its contractual obligations and the requirements of applicable data protection laws. In addition, Frontify shall immediately take reasonable measures to contain, investigate and mitigate the security incident.

14. Regular review, assessment, and evaluation

Frontify implemented a procedure for regularly examining, assessing, and evaluating the effectiveness of the technical and organizational measures to ensure the security of processing. This includes an assessment process and a contract control process.

14.1. Assessment process

Measures to ensure that data is processed securely and in accordance with data protection regulations.

Description of the assessment process:

- data protection management
- formalized processes for data protection incidents

- documentation of customers' instructions
- formalized order management
- service level agreements

14.2. Contract control process

Measures to ensure that data is processed according to the instructions of the customer.

Description of the contract controls:

- clear contract drafting
- documentation of customers' instructions
- formalized order management

Frontify

privacy@
frontify.com