Privacy Notice

Version March 12, 2026

1. Introduction

Frontify AG (“Frontify” or “We”) is a Swiss company that provides a cloud-based brand management Software-as-a-Service (“Platform”) to professionals and companies. Headquartered in St. Gallen, Switzerland, Frontify has subsidiaries in Frankfurt (Germany), New York (USA), London (UK), and Paris (France).

The Platform is a customizable solution for every specific brand requirement and is designed to maximize brand consistency through centralization. Frontify offers a wide range of features, including but not limited to the Brand Guidelines, the Digital Asset Management, the Creative Collaboration, and the Digital & Print Templates. Additionally, the Platform is an intuitive solution that enables every user to upload and centralize digital assets independently, define brand essentials with dynamic guidelines, build a design system for digital efficiency, and create customized templates for on-brand marketing material.

2. What does this Privacy Notice regulate?

This Privacy Notice describes how Frontify Processes Personal Data of individuals (“You”) who visit frontify.com or other websites operated by Frontify (as defined in section 5.20), use the Platform, participate in marketing events, brand summits, or other initiatives organized by Frontify (“Frontify Events”), and/or apply for a vacancy.

Frontify respects everyone’s privacy rights and applies the highest standards of data protection regardless of the user’s location. We’re committed to complying with all applicable laws and regulations globally.

We update this Privacy Notice regularly and make the latest version available on the Site, with a date of last revision.

3. Definitions

For the purpose of this Privacy Notice, the following definitions apply:
”Personal Data”, “Data Subject”, “Processor”, “Controller”, and “Processing” shall have the meanings provided by the EU GDPR.
Additional terms shall have the meaning provided by us in this Privacy Notice.

4. How does Frontify qualify with respect to the Personal Data Processed?

In the context of the services provided to our customers under the applicable agreement - which includes the General Terms and Conditions for Enterprise Customers ("GTC") and the Data Processing Agreement ("DPA") - Frontify qualifies as a Processor. We Process Personal Data of Platform users on behalf of the customer and in accordance with the terms of the DPA. The customer determines who shall be authorized to access their Platform environment and is primarily responsible for the Processing of the users' Personal Data.

Frontify may also carry out processing activities that qualify it as a Controller. This applies to all processing activities in which Frontify independently determines the purpose and means of Processing Personal Data. In such cases, every request received by a Data Subject is handled by Frontify.

To ensure transparency of information, We disclose the purpose and lawful basis applicable to each Processing activity in section 5 below. Frontify acts as a Controller for each Processing activity listed in section 5, except for section 5.1, 5.13 (solely with regard to Customer Hub), and 5.16, where Frontify acts as a Processor.

5. Which Personal Data does Frontify Process?

In this section, You can find relevant information about the different Processing activities We perform. This includes information about the purpose and the lawfulness of the Processing.

5.1. Platform user information

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 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.

Lawful basis: Frontify Processes the Platform user information as a Processor. The customer, who qualifies as a Controller, is responsible for the lawfulness of Processing towards the Data Subjects.

5.2. Contact information of Site visitors

To subscribe to services available on our Site (e.g. newsletters, webinars, demo, Frontify Events, etc.), You may provide certain contact information by filling in online forms or by using our chatbot ("Contact Information"). Depending on the service You request, We might ask You to provide some of following information:

- Name
- Work email address
- Phone number
- Company name (and other company-related information)
- Job title

We may enrich the Contact Information with Personal Data We receive from other sources, such as third-party providers of business information and publicly available sources (like social media platforms). This may include physical mail addresses, job titles, email addresses, phone numbers, IP addresses, and social media profiles. This helps us update and improve our records, identify new customers, create more personalized advertising, suggest products and services that may interest You, deliver personalized communications and promote events. The collection of Your Personal Data by these other third-party providers is governed by such provider's privacy policy.

Lawful basis: We rely on our legitimate interest in providing You with the services You subscribed to, and also sending you personalized marketing communications. We may retain Personal Data processed for this purpose until You unsubscribe from our services or there is no longer a legitimate interest of Frontify in Processing your Personal Data.

5.3. Site visitors' usage and statistics information

We use different tracking technologies (e.g., cookies, pixels, events, tags) to analyze how visitors interact with the Site, including collecting statistics about the use of certain features ("Site Visitor Information"). This helps us improve the quality, design, and performance of our Site, and to use it for our marketing communication. Site Visitor Information is Processed in an aggregate and anonymous form, unless You submit Contact Information as stated in section 5.2.

Site Visitor Information might contain the following:

- IP address
- geographical location
- browser type and version
- ISP information
- referral website source
- length of visits
- pages viewed
- language preferences
- download history
- conversation data with Our chatbot
- operating system

We use different types of cookies. Technical cookies are needed for the functionality and improvement of Our Site (e.g., identify visitors, keep preferences), while statistics and marketing cookies allows us to customize our online services and improve the visitor's experience accordingly.
Except for strictly necessary cookies that are always active, You can decide which categories of cookies You want to activate, and which should remain off. The cookie banner displayed on the Site enables You to make Your choice when accessing the Site, and to get more details about cookies' purposes. Additionally, You'll be able to manage Your cookie settings at any time by clicking on the relevant button displayed on the left-bottom-side corner of the Site.
You can learn more about how the types of cookies We use and their purposes, and how to manage Your cookie preferences in Our Cookie Policy.

Lawful basis: Frontify relies on the consent of Site visitors to activate non-essential cookies. With regards to essential cookies, Frontify Processes such Personal Data based on Frontify's legitimate interest to run the Site.

5.4. Billing information

For billing purposes, We may collect and use the following Personal Data if the contractual party is a natural person:

- Name of customer
- Customer's credit card information
- Billing address

We neither collect nor store any credit card information ourselves. We use payment services providers, namely, Zuora, and Adyen.

Lawful basis: The Processing of billing information is necessary for the performance of the applicable contract to which the customer is a contractual party.

5.5. Product research

5.5.1. Analytics Insights

We use aggregated analytics insights (anonymised and/or pseudonymised data) collected through Amplitude regarding how Platform users interact with the Platform ("Analytics Insights"), to support our research efforts in improving our Platform performance and user experience. This information may include:

- Platform users' interactions with the Platform interface (e.g., clicks)
- Metadata related to such interaction (e.g., page ID, usage of filters, format type)
- Technical information about the device and browser used (e.g., screen size, operating system, browser type)
- Metadata related to the session (e.g., duration, feature usage)

In addition, the same aggregated analytics insights are used to identify behavioral patterns and define user groups (e.g., "admins"), which may be synced with our in-app support functionality to trigger invitations to voluntary research activities.

Lawful basis: We rely on our legitimate interest in improving our services and delivering the best user experience.

5.5.2. Surveys

To further support our product research and development support, We may invite You to participate in interviews, surveys, or other experimental studies and provide us with Your feedback ("Product Research Data"). Product Research Data may contain the following Personal Data:

- Name
- Email address
- Position
- Company
- Audio, video, and desktop recordings
- Content of feedback

If You intend to participate in one of our product research activities, We will ask for your prior written consent. The Personal Data collected in the context of such research activities will remain confidential. If We plan to use Product Research Data for other purposes than those set out above (e.g. publish parts of the Product Research Data), We will ask for Your specific consent beforehand or will only do so if the Product Research Data is anonymized.

Lawful basis: We rely on Your informed consent to collect and Process Product Research Data as outlined in each relevant consent form.

5.5.3. NPS surveys

In order to be able to continuously improve our services, We may invite You to participate in NPS surveys to measure your satisfaction using the Platform and other services ("NPS Survey Data"). NPS Survey Data might contain the following Personal Data:

- Name
- Email address
- Geographical location (inferred from survey answers)
- Company
- NPS score
- Content of feedback

After completing the NPS survey, We may contact You to get more details about Your feedback or ask You to leave us a review on one of our trusted third-party review platforms. The Personal Data collected in the context of such surveys will remain confidential. If We plan to use the NPS Survey Data for other purposes than those set out above (e.g. including your feedback in marketing and promotional materials to highlight customer experiences and support our overall brand messaging), We will ask You for your specific consent beforehand, or would only do so if the NPS Survey Data is anonymized.

Lawful basis: We rely on Your consent to Process NPS Survey Data.

5.5.4. Amplitude Session Replay for Beta features

As part of our product research and development efforts, we may also use Amplitude Session Replay to evaluate and improve new Beta features. Amplitude Session Replay allows us to reconstruct how Platform users interact with new platform functionalities and identify opportunities for improvement. For clarity, Amplitude Session Replay does not record video of Platform users and allows for the masking or exclusion of any confidential or Personal Data.

In addition to the standard Analytics Insights described in section 5.5.1 above, the information collected through Amplitude Session Replay may include:

- Additional interaction signals (e.g., navigation and scrolling)
- Any Personal Data voluntarily entered into the Platform during the session is masked (e.g., uploaded images or videos; text inputs).

Amplitude Session Replay is activated only for the duration of a customer's use of a Beta feature and is available only on customer instances where explicit, written informed authorisation has been provided by the customer's administrator. Such authorisation may be withdrawn at any time. Session Replays are automatically deleted after 30 days of collection.

Lawful basis: We rely on our legitimate interest in improving new functionalities before official release and delivering the best user experience. The authorisation to enable Session Replays on a specific customer's instance is granted by the customer's administrators.

5.6. Commercial research

In order to assess customer satisfaction using our Platform, including analyzing Frontify's post-implementation impact, and enable data-driven and customer-centric commercial strategies, We may invite You to participate in interviews, surveys or other experimental studies and give us Your feedback ("Commercial Research Data"). Commercial Research Data might contain the following Personal Data:

- Name
- Email address
- Position
- Company
- Audio, video, and desktop recordings
- Content of feedback

If You intend to participate in one of our commercial research initiatives, We will ask for your prior written consent. The Personal Data collected in the context of such research activities will remain confidential. If We plan to use the Commercial Research Data for other purposes than those set out above (e.g., use your answers for quotations in marketing and promotional materials to highlight our customers' experience and support our overall brand messaging), We will ask for your prior written consent beforehand, or would only do so if the Commercial Research Data is anonymized.

Lawful basis: We rely on Your consent to Process Commercial Research Data.

5.7. Marketing communications

Depending on whether You are a Site visitor, a Platform user or a participant to a Frontify Event, We may send You marketing material that We believe may be of interest to You. This may include, but is not limited to marketing campaigns, product updates, news about future Frontify events, webinars, and newsletters. You can also subscribe to our newsletter to receive regular product updates, brand-related content, and general insights. You may unsubscribe from any communication at any time by using the relevant link included in each email. We will not share your Personal Data with third parties for their marketing purposes.

Lawful basis: We rely on our legitimate interest in promoting our services and providing You with the best possible user experience.

5.8. Customer testimonials

Subject to your consent, We may publish customer testimonials, which may include Personal Data, on the Site or use them in other marketing materials. You may withdraw your consent at any time by using the contact details in section 12.

Lawful basis: We rely on your consent to publish customer testimonials.

5.9. Frontify Events

If You register for or attend a Frontify Event, We may process Your Personal Data to manage registration, ticket purchase, attendance, and related logistics. This may include Processing payments, issuing invoices, managing refunds, and sending event communications (e.g., schedules or important updates).

Frontify Events may involve photography and videography. Images or recordings of participants (individually or as part of the audience) may be used for Frontify's promotional purposes, including but not limited to posting on its social media channels. We will not use such materials for other purposes, unless we have obtained Your prior informed and explicit consent, where required.

With Your explicit consent, We may share your contact details and company information with event sponsors and/or enable sponsor communications. If You opt into the attendee networking feature during registration, Your LinkedIn profile URL may be shared with other attendees for networking purposes.

Lawful basis: We process Your Personal Data for the performance of a contract (event participation), based on our legitimate interests in organizing and promoting our events, and/or based on your consent where required.

5.10. Recruiting practices

5.10.1. Job candidates' profiles

If You apply for a vacancy at Frontify, We will process any information that You provide us, as well as information that is publicly available (e.g., Your LinkedIn profile), only for the purpose of evaluating You for a job position and for the time necessary to fulfill that purpose. Job candidates' Personal Data might contain the following:

- Name
- Email address
- Contact information
- Education and professional background records

Sometimes, We may want to retain job applicants' profiles for longer periods - for instance, when We believe that a candidate may be assessed for different job opportunities simultaneously - in which case, We request their prior written consent. We use a trusted third-party tool ("Lever") to store and update all candidate profiles. If We decide not to move further with any application, and absent candidates' consent to keep their profile in our talent pool (see section 5.11 of this Privacy Notice), We will delete or anonymize their Personal Data within 30 days.

Lawful basis: We rely on our legitimate interest in recruiting new employees.

5.10.2. Frontify talent pool

We are always looking for the best talents in different fields of expertise. Thus, to speed up our recruiting process and keep track of top-performing candidates, We maintain a talent pool database, by using a trusted third-party tool ("Lever"). Upon their application, all potential members can join the talent pool directly through the system, or, in other cases, provide their consent after being contacted by our Employee Success Team. Upon receipt of your consent, We will store Your information for one year. If Your initial application was unsuccessful, We will contact You for any new job opportunities that may arise during that one-year period and for which We believe You may be suitable. You have the right to request, at any time, a copy, correction or deletion of Your Personal Data by using the

contact details in section 12 of this Privacy Notice. Within 30 days of Your request to delete your data, We will anonymize or delete Your Personal Data. Furthermore, at the expiry of each year following your initial consent, You will be able to either renew Your authorization for one additional year or to request deletion of Your profile from our talent pool, by following the relevant instructions provided to You via the talent pool.

Lawful basis: We rely on your consent to store your application data in the talent pool as outlined above.

5.10.3. AI-Assisted recruiting

As part of our recruitment process, we use third-party artificial intelligence (AI) tools to support our hiring activities. These providers are vetted for security and compliance purposes prior to engagement and are subject to data processing agreements that impose appropriate data protection and security obligations.

AI tools may be used to: i) record and transcribe interviews; ii) assist our recruitment team in reviewing and organizing candidate profiles and application materials; iii) support the internal evaluation process. They serve solely the purpose of assisting our recruiters in documentation and review processes and do not replace human judgment. All candidate assessments and final hiring decisions are made exclusively by our recruitment team.

Where interviews are recorded and transcribed using AI tools, candidates may opt out of AI-assisted recording and transcription prior to the interview without any negative impact on their application or consideration for employment. In such cases, alternative arrangements will be made.

Depending on the tool used, Personal Data Processed may include identification and contact details, professional information contained in your application, and audio and transcription data from interviews. We implement appropriate technical and organizational measures to ensure that Your data is handled securely and in accordance with applicable data protection laws.

We do not use AI tools to make solely automated decisions that produce legal or similarly significant effects concerning candidates.

Lawful basis: We rely on our legitimate interest in conducting an efficient recruitment process, and where required, your consent for the recording and transcription of interviews.

5.11. Calls recording

For the purpose of coaching our commercial teams in handling external calls, improving our customer service and inform our product team about new features requested by our customers, We may record calls with prospects, clients and other partners, using a third-party provider. If You participate in these calls, You'll have the opportunity to consent or decline the call recording, by selecting the relevant option before the meeting starts.

All recordings are automatically deleted after a three-year period. During such storage timeframe, recordings are made accessible only to those employees who have a clear need-to-know the information due to their position. Upon request, recordings can be shared with any participant to the call, who can also request at any time to delete or anonymize the recording by using the contact details in section 12.

Lawful basis: We rely on Your consent to record calls for the purposes set out above.

5.12. Frontify academy

The Frontify academy provides a comprehensive online learning environment where users can engage in courses and certification programs aimed at deepening their understanding and expertise in utilizing the Frontify platform. It is run by a third-party provider called Sana Labs AB ("Sana"). Interested individuals who want to join the Frontify academy need to log-in to the platform of Sana, which is the Controller of the personal data of its users. In order to create an account, users might need to provide the following personal data:

- Name
- Email address

However, for full details about what kind of Personal Data is Processed on Frontify academy and how it is used We recommend consulting the privacy policy of Sana. Sana's privacy policy can be accessed here and is also linked during the log-in procedure.

Lawful basis: Sana in its role as a Controller is responsible for the lawfulness of Processing towards the Data Subjects.

5. 13 Frontify Customer Hubs / Portals

The Frontify Customer Hub serves as an integrated online resource center, providing Platform users with onboarding guidance, training resources, and account management capabilities throughout their customer journey. Authorized Platform users can seamlessly access the Customer Hub from within the Platform according to role-based permissions. In

addition, Frontify offers its partners the opportunity to join the Partners Hub for training, certification, and enablement resources. Both the Customer Hub and the Partners Hub are operated by a third-party provider called EverAfter AI Ltd. ("EverAfter").

In order to offer the Customer and Partners hubs, the following Personal Data of authorised users is collected and used:

- Name
- Email address
- Scheduling information & Google Calendar info (meeting preferences, availability)
- Company name
- Frontify user role
- Unique User IDs
- Legal contact
- Billing contact

More specifically, scheduling and Google Calendar information, while not mandatory to benefit from the Customer Hub services, may be processed to enhance the Platform user experience. The Google Calendar integration syncs meeting details between Frontify and customers (such as meeting title, agenda, participants' names and emails, and dates), while the Gong integration enables recordings of video calls to be made available to meeting participants. This information (including name, email, notes and recordings) is accessible only to invited participants and helps provide transparency, track interactions, and review key meetings (e.g. training sessions) on demand. Customers may request to disable meeting recordings or remove the meetings overview section from their Customer Hub at any time.

Meeting details and recordings processed through these integrations remain stored within the respective third-party providers' systems (e.g., Google and Gong) and are subject to their applicable hosting locations, security measures, and retention policies. Data hosted within EverAfter's infrastructure is stored within the European Union via EverAfter's EU-based infrastructure and retained for the term of the applicable customer or partner agreements. Upon cessation of the Customer/Partner hub services, all Personal Data is deleted within ninety (90) days.

Lawful basis: We Process the Platform user's Personal Data as a Processor to fulfil our contractual obligations in providing our customers with onboarding and enablement resources. Our customer, who qualifies as a Controller, is responsible for the lawfulness of Processing with respect to Data Subjects.
For Partner data processed through the Partner Hub, we rely on legitimate interests in

maintaining and supporting our partner ecosystem to enhance service delivery to our customers.

5.14 Customer feedback and ideas

We always encourage our customers, partners, prospects and Platform users to share their insights, ideas and requests to help us improve Our Platform and services. Everyone can send us their feedback by clicking “submit idea” and filling in the form available on our Site, or by communicating their ideas to the responsible Customer Success Manager or our support team who will circulate the feedback internally. In either case, to follow up on Your request or to process Your idea in our product roadmap, We might collect the following Personal Data:

- Name
- Email address
- Position
- Company
- Content of feedback

Lawful basis: We rely on Frontify’s legitimate interest in improving its Platform and services and providing the best user experience.

5.15 Frontify Marketplace

We offer our customers the possibility to access and use the Frontify Marketplace, which is integrated and part of the Platform. The Frontify Marketplace is the online directory or catalog of software applications, plugins, and extensions, that users may activate to enhance their experience through the Platform. Given that the Frontify Marketplace is available on the Platform, users can access it using the same unique credentials that allow them to enter the Platform (see section 5.1).

If You choose to activate a third-party app, You authorize the third-party app provider to access and use any of Your Personal data in accordance with the third-party app provider terms and acknowledge that Frontify will have no liability in regard to any Processing of Your Personal Data by a third-party app provider.

Lawful basis: The relevant third-party app provider is Controller of the Personal Data and responsible for the lawfulness of Processing towards the Data Subjects.

5.16 Frontify AI capabilities

We offer a range of AI-enabled capabilities within our Platform designed to streamline asset management and support brand consistency. They include both in-house-developed AI functionalities (AI Features) and third-party AI services and Add-ons that can be integrated with the Platform at the Customer's request (Third-Party AI services), as listed below.

Frontify AI Features:

- Enhanced Image Search: An AI-enhanced search capability that automatically understands what an image depicts and makes it searchable using natural language, even if the asset doesn't have manual tags or metadata.
- Automatic Asset Processing:
    - Auto Tagging: A feature that automatically generates suggested tags for assets based on their content, reducing the need for manual metadata entry.
    - Asset Content Search (OCR Search): A feature that analyses documents (pdf, docx, and pptx) and images (png, jpeg, tiff) in Your projects and libraries to extract and index any text content to improve searchability.
- Brand Assistant: A conversational AI assistant embedded in your brand portal that lets users ask questions about brand guidelines and receive immediate, brand-compliant answers.
- AI Translation: An AI-powered translation functionality that instantly translates brand guideline pages into other languages, preserving formatting and structure. This helps global teams access and understand brand content in their own language.

Third-Party AI Services:

- Apps and integrations: additional AI capabilities are supported through third-party apps and integrations, including automated image generation, metadata translation, and background removal.
- Automations: a functionality that allows You to simplify workflows and reduce manual effort by setting up rule-based actions. While certain core automation actions are available by default, additional OpenAI-powered actions can be used by installing a dedicated app from the Frontify Marketplace. Automations are configurable, and users can enable/disable specific AI automation actions.

The data Processed in the context of the above AI features include the following categories and purposes:

- For Enhanced Image Search, Automatic Asset Processing
  - Data categories:
    - Asset content
    - Extracted text from documents/Images via Optical Character Recognition (OCR)
    - Search queries
  - Purpose:
    - Improve asset discovery, making search results more relevant
    - Suggest metadata/tags for assets
    - enable semantic search, including natural-language queries

- For Brand Assistant
  - Data categories:
    - Asset content
    - Guideline content
    - User prompts and generated output
  - Purpose:
    - Provide users with guidance on brand compliance and help them find relevant assets

- For AI Translation:
  - Data categories:
    - Guideline text submitted for translation
  - Purposes:
    - Provide automated translation to support multilingual brand governance

- For Apps and Integrations, Automations:
  - Data categories:
    - User input (e.g., textual prompts, asset content, metadata, or other info)
  - Purposes:
    - Generate output according to users' instructions

  Processing activities depend on the specific app and integration, and how the automation is configured by the Customer.

To provide the above AI functionalities, We rely on AI technology from trusted third parties, such as AWS and Microsoft Azure AI. In doing so, we ensure responsible and compliant data use, as described further below.

None of the offered AI Features requires the Processing of Personal Data to operate. Notwithstanding, Personal Data may be accidentally or voluntarily included in user prompts, and/or embedded in customer guidelines or asset data. To address these circumstances, we ensure that necessary data protection agreements are in place, including all required safeguards to adequately protect data in accordance with applicable laws.

Data Processed by third-party AI providers is not subject to additional processing than what is strictly necessary to provide their services to us. As a result, no data is used to train or fine-tune large language models (LLMs), nor is it shared with other third parties. Additionally, data minimisation measures are applied to ensure data processed is not retained by the third-party AI provider longer than necessary to achieve the relevant purpose.

Individuals whose personal data is processed within or alongside AI features may exercise their rights under the GDPR (access, correction, deletion, restriction, objection) in accordance with section 10 below.

Where applicable, AI assistance or auto-generated content is identified or labeled in the user interface (e.g., recommended tags, translation suggestions). Additionally, users can review, edit, accept, or remove AI-suggested metadata.

The AI features are evolving; therefore, some of the above mentioned capabilities may be in development or beta form.

Lawful basis: Any processing of personal data by us to provide the Frontify AI Features is performed in our capacity as Processor. Our customers who qualify as Controllers are responsible for the lawfulness of Processing with respect to Data Subjects.

5.17 Video surveillance

To help protect the safety and security of our Swiss office premises, We have installed Arlo Secure surveillance cameras at building entrances. These cameras operate continuously but record only outside of business hours. The purpose of this monitoring is to deter and detect unauthorized access, theft, vandalism, or other security-related incidents, based on our legitimate interest in ensuring property and personnel safety. The cameras may record

video and audio of individuals entering or near the premises, including employees, visitors, and other third parties. We do not use facial recognition or other biometric technologies. Recorded footage is securely stored in the Arlo cloud environment, hosted by Amazon Web Services (AWS) in Dublin, Ireland, and is retained for a maximum of 30 days. Access to the footage is restricted to authorized personnel on a strict need-to-know basis, with approval from our Security team. We act as the data controller for this processing, in accordance with the Swiss Federal Act on Data Protection (FADP) and, where applicable, the General Data Protection Regulation (GDPR).

Lawful basis: We rely on Frontify's legitimate interest in ensuring property and personnel safety.

5.18 Special categories of Personal Data

Frontify does not process any special categories of Personal Data as defined under Art. 9 (1) GDPR. Therefore, We never ask our existing and/or prospective customers to provide Personal Data revealing their racial or ethnic origin, their political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation. If We become aware that We received any such information from a user and/or customer, We act promptly to inform the latter, gather relevant consent and/or remove that information.

5.19 Personal Data of children

Our Platform is intended for business purposes and not for use by individuals under the age of sixteen, so We do not knowingly collect information from anyone under that age. If We become aware of receiving information from an individual under that age, We take immediate steps to delete such information.

5.20 Frontify's websites

Frontify operates the following websites (each a "Site"):

- frontify.com
- help.frontify.com
- brand.frontify.com
- paradigms.frontify.com
- paradigms.io
- weare.frontify.com/d/G1bTDvE5HuEK
- developer.frontify.com
- ventura.frontify.com

The Personal Data processed in the context of the mentioned websites are mainly Site Contact Information (section 5.2) and Site Visitor Information (section 5.3) as described above. For a detailed list of cookies deployed on each of these websites, please check Our Cookie Policy.

6. How long does Frontify retain Personal Data?

We retain Your Personal Data for as long as it is necessary to fulfill the purpose for which it was collected. To ensure this, We have defined time frames, after which the data is deleted.

Besides that, You can reach out to us at any time using the contact details in section 12 and request deletion of Your Personal Data. Further information about how You can exercise Your privacy rights are included in section 10.

7. Where does Frontify store Personal Data?

The customer data, including Personal Data, is hosted on secure server locations of AWS, either in Europe or in the USA, depending on the customers' preference. Generally, and if not otherwise selected by the customer, We tend to store the data of our European-based customers in Europe and the data of our non-European-based customers in the USA. Additionally, We might also Process Personal Data in our office locations in Switzerland, France, Germany, UK and the USA.

8. Does Frontify engage with third parties?

8.1. Service providers used as Subprocessors

Whenever we Process Personal Data on behalf of our Customers in the provision of the Frontify Services under the customer agreement, we act as a Processor. In this context, we engage selected third-party service providers to support the delivery of the Platform, such as cloud hosting and infrastructure providers. These providers qualify as sub-processors. Customers may consult the current list of subprocessors, including a description of the processing activities performed, in our DPA, available here. We update this list from time to time and notify Customers of changes in accordance with the terms of the DPA.

8.2 Service providers used for our own business operations

Whenever we Process Personal Data for our own business purposes, we act as a Controller. In this context, we engage trusted third-party service providers to support our internal operations and business activities. These may include, but are not limited to, providers of: i) Customer relationship management (CRM) systems; ii) Marketing automation and attribution tools; iii) Internal collaboration, documentation, and productivity tools; iv) Security monitoring and fraud prevention services; and v) Business analytics and performance measurement tools.
They are engaged for several purposes. The most relevant can be summarised as follows:

- Sales and commercial operations
- Billing and subscription management
- Recruiting and hiring practices
- Marketing and demand generation
- Customer support and relationship management
- Internal communication and collaboration
- Business analytics and performance optimization
- Support services improvement and knowledge base management
- Product research, analysis and development

In providing their services to us, our service providers may Process some of Your Personal Data. In such cases, we apply data minimisation measures, including anonymisation or pseudonymisation wherever possible, to ensure that providers access only the minimum categories of data required to provide their services to us. In certain cases, such as where You include Personal Data or confidential information in a support request, further minimization may not be possible. In such instances, the information is processed solely as necessary to respond to your request, document troubleshooting steps, investigate incidents, and improve our services and knowledge base.
Service providers Process Personal Data on our behalf and under our instructions, pursuant to appropriate data processing agreements in accordance with Article 28 GDPR. Where Personal Data is transferred outside the EEA, Switzerland, and/or UK, we ensure that appropriate safeguards are implemented in accordance with the applicable data protection laws, including Standard Contractual Clauses or reliance on an adequacy decision, as applicable.
If service providers use AI-enabled or automated tools to provide services to us, such use is governed by the same contractual safeguards and is strictly limited to the purposes described above. Personal Data processed in this context is not used to train general-purpose AI models or for any independent or unrelated purposes.

9. Does Frontify perform international data transfers?

We may transfer Personal Data outside of Switzerland and the European Union. In such cases, We guarantee that data are handled by trustworthy vendors in accordance with the applicable data protection laws. The transfer of Personal Data outside of the EU may concern countries deemed by the EU Commission to provide an adequate level of data protection according to Art. 45 GDPR ("Safe Third Countries"), but also other countries. In these circumstances, We implement appropriate safeguards as required by Art. 46 GDPR (e.g. EU Standard Contractual Clauses, "EU SCC"). To the extent that Swiss or UK data protection laws require additional safeguards, We implement such in accordance with the instructions of the Swiss Federal Data Protection and Information Commissioner, and the Information Commissioner of the UK.

10. How can I exercise my privacy rights?

Subject to the applicable data protection laws, You may have the following rights:

- the right to access and request copies of Your Personal Data
- the right to rectify Your Personal Data
- the right to request deletion of Your Personal Data
- the right to restrict the processing of Your Personal Data
- the right to request the transfer of Your Personal Data.
- the right to object to the processing of Your Personal Data
- the right not to be subject to automated individual decision-making, including profiling.

If You wish to exercise Your rights with respect to Your Personal Data or raise a complaint about how We Process Your Personal Data, You can contact Us using the contact details in section 12. We'll respond to Your request as soon as possible, and in any case not later than 30 days of receipt of your request . Also, You have the right to lodge a complaint with the competent data protection authority in Your country or where Frontify operates.

If You wish to unsubscribe from any communication You receive from Frontify (e.g., newsletters or marketing emails), You may use the "unsubscribe" link included at the bottom of our emails.

As a Platform user (see section 5.1), You can either exercise your rights listed above by using the functionalities of the Platform (e.g. adjusting your profile settings) or by contacting the relevant Controller (which is normally the company which grants You access to the Platform, e.g. Your Employer). In case We receive a request from You regarding Personal Data

that We use as a Processor, We will forward such request to the respective Controller or advise You to contact the relevant Controller of Your Personal Data pursuant to Art. 28 (3) (e) GDPR.

Please note that, limiting or objecting to some Processing of Your Personal Data may prevent You from engaging in certain Site activities or impact Your online experience when working with the Platform.

11. Which rights do I have as a California resident?

If You are a California resident and We process Your Personal Data, the California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act of 2020 (collectively, the "CCPA") may apply to Our processing activities. The requirements of the CCPA substantially overlap with existing obligations under the GDPR, therefore, they have been addressed throughout this Privacy Notice.

This paragraph supplements the information provided in this Privacy Notice with certain complementary and/or additional rights that California residents are specifically entitled to under the CCPA.

For clarity, certain CCPA terms correspond approximately to GDPR terminology as follows:

GDPR	CCPA
Personal Data	Personal Information
Controller	Business
Processor	Service Provider / Contractor

We list below Your rights as a Californian resident under the CCPA:

- Right to know: The right to request information about the categories of Personal Information We have collected about You and the purpose of collection.
- Right to delete: The right to request deletion of your Personal Information, subject to certain exceptions, including where retention is necessary for providing Our services to You, compliance with legal obligations, or other purposes permitted under the CCPA.
- Right to correct: The right to request the correction of inaccurate information that We maintain about You.

- Right to limit the use and disclosure of sensitive Personal Information: The right to direct Us to limit the use and disclosure of Your sensitive Personal Information to purposes permitted by the CCPA. However, We do not Process sensitive Personal Information as stated in section 5.18 of this Privacy Notice.
- Right to opt-out of sale or sharing: the right to opt out of the sale or sharing of Your Personal Information. However, We do not sell or share Personal Information as those terms are defined under the CCPA. For clarity, "selling" under the CCPA refers to, transferring or making available of Personal Information to a third party for monetary or other valuable consideration; whereas, "sharing" refers to disclosing Personal Information to a third party for cross-context behavioral advertising.

You may submit any request concerning the CCPA to Our privacy team, using the contact details provided in section 12 below. Once We've verified Your identity, Your request will be answered promptly, within 45 days. If additional time is required, We will notify You of the extension and the reason for it, in which case the total response period shall not exceed 90 days.

We'll not discriminate You for exercising any of Your rights under the CCPA or any other applicable data protection legislation.

12. How can I contact Frontify for privacy matters?

Please find here our contact information:

Frontify AG

Unterstrasse 4

9000 St. Gallen

Switzerland

Email address: privacy@frontify.com

If You have any privacy-related questions or You want to exercise Your privacy rights, You can write an email to privacy@frontify.com at any time.

We'll respond to Your request as soon as possible but latest within 30 days.

13. Does Frontify have a representative in the EU?

Frontify Deutschland GmbH is the representative of Frontify AG in the EU. Please find below the contact details:

Frontify Deutschland GmbH
Friedrich- Ebert- Anlage 36
60325 Frankfurt am Main
Email address: privacy@frontify.com

14. Where can I find more information about Privacy at Frontify?

Our Privacy FAQ provides our customers and platform users with relevant information about how Frontify handles their personal data, and which steps We take to ensure ongoing compliance with data privacy laws and regulations.

The Frontify DPA defines the rights and obligations of Frontify in its role as Processor and of the customer in its role as Controller of the customer personal data processed in the course of providing the Frontify Services. In our Frontify DPA You can also find the subject matter and details of processing (Exhibit A), the sub-processor list (Exhibit B), and the technical and organizational measures (TOMs).

The Cookie Policy provides You with information about the use of cookies on Our websites as well on Our Frontify Platform.

This Privacy Notice was last reviewed and updated on March 12, 2026.