Bynder Global Privacy Policy

This Global Privacy Policy describes Bynder's commitment to protecting your privacy. Under this Global Privacy Policy, we are informing you on how Bynder handles data as a Controller, meaning all data we process for our own purposes. Where Bynder is a Processor of data, that activity is governed by a Data Processing Agreement entered into between us and the Controller of the data.

An increasing number of jurisdictions are enacting privacy laws providing individuals with privacy rights. The predominant privacy laws with regard to Bynder's business are the GDPR, UK GDPR, and CCPA/CPRA.

Scope

Bynder BV and its related entities and subsidiaries, including Bynder LLC, Bynder Limited, and Bynder Pty Ltd (ACN 656 251 213), Bynder Software SL, Bynder Sofware FZ LLC and Bynder GmbH ("Bynder"), are an international group of companies (we / us / our) offering a cloud-based digital assets management Software-as-a-Service to companies.

In relation to the operation of our business, Bynder may collect data on you directly from you or from third parties, from publicly available sources, or automatically (through the use of cookies or other tracking technologies) for the purpose of marketing our services, supporting our own business purposes or performing our legal and contractual obligations (access to our online services, customer support, considering applicants for employment by a Bynder entity). When we process usage data and account information, we are acting as a Controller. When we process data and content uploaded or managed in the products by our Customers or generated by the products on behalf of our Customers (also referred in our agreement with Customers as "Customer Data" or "Customer Content"), we are acting as a Processor and subject as such to the Data Processing Addendum in place with our Customers.

This privacy policy applies to all Processing of Personal Data carried out by us as a Controller in the context of carrying out our business (with the exception of internal employment related processing).

Definitions

Controller: the entity which determines the purposes and means of the Processing of Personal Data.
Customer: the legal entity/entities which, being a party to an agreement with Bynder, purchases the products and/or services offered by Bynder.
Data Subject: the identified or identifiable person to whom Personal Data relates.
Job Applicant: the natural person who replies to a job advertisement, submits an application in response to an advertisement or engages otherwise with Bynder's hiring and recruitment process.
Personal Data: any information relating to an identified or identifiable natural person.
Processing: the most general definition of Processing embraces any action taken which involves Personal Data, i.e. data related to an identified or identifiable individual (Data Subject). This may include such action as storage, consultation, analysis, pseudonymization, deletion.
Processor: the entity which Processes Personal Data on behalf of the Controller.
User: any individual who accesses and/or uses the products and/or services offered by Bynder through Customer's account.

Details of Processing Operations

How do we collect the data?

- **Directly from you** when you request information, respond to a survey, enter into a business relationship, use our products, contact us, apply for a job.
- **Automatically** when you visit our websites, receive a marketing email or use our products. Our cookies and other tracking technologies are discussed in more detail here.

- **From third party sources**, including publicly available databases or third parties from whom we have purchased data.

What are the categories of Data Subjects?

- Individuals employed by or representing, in one way or another, Customers and partners with whom Bynder has entered into a contractual relationship with respect to the development and/or the provision of the services and the products
- Users of the cloud-based services
- Individuals employed by or representing, in one way or another, prospective Customers or partners
- Job Applicants
- Website visitors

Our website and products and services are for business use and are not intended for or targeted toward children under the age of 16 (“Children”). We do not knowingly collect any information about Children. We encourage parents and legal guardians to monitor the internet usage of their Children and ensure they do not provide personal information to Bynder. If you believe that we have collected information about Children, please contact us at **privacy@bynder.com** so that we can delete the information.

What categories of Personal Data we may process?

- **Prospect and Customer/partner information**: name, email address, phone number, job title, professional backgrounds, communication and responses, billing information and other information related to establishing and maintaining a relationship between you and us.
- **Data we collect automatically** (when you visit our websites, receive marketing emails or use our products): device information (IP address), device attributes (e.g. hardware model, unique device identifiers and characteristics, operating system, web browse type and version), connection information (ISP information, browser type, language and time zone), website page views, access date and time, heat mapping, conversion

and click tracking. Our cookies and other tracking technologies are discussed in more detail here.

- **User data**: login information (name, email address and password), log data (address and names of web pages and files accessed, date and time of access, volumes transferred and originating IP addresses), usage data (including features of the services used, service configuration setting (storage), crash logs, access time, profiles with User-related information).
- **Survey data and Customer testimonials**: opinions on the current state of our services, opinions on future functionality and the direction of our product offering.
- **Job Applicant details**: name, title, email, address, telephone number, emergency contact, beneficiary information, data related to your professional experiences and personal interests, information in resume, cover letter, or other materials collected as part of previous or current applications. Depending on the Job Applicant's jurisdiction, potentially sensitive information including race, ethnicity, national origin, health (medical condition, health, sickness records), data related to criminal convictions and offenses may be collected as well.

Details of the purposes:

What are the purposes of this Processing and the legal basis for such Processing?

In the following, we are describing the purposes for which your Personal Data is processed. If you are a resident in the EEA, Switzerland or UK, the lawfulness of that Processing will depend on the Personal Data concerned and the specific context in which we collect it. Where we are Processing your Personal Data for our own purposes, we normally rely on our legitimate interest to do so (art. 6 (1) (f) of GDPR), except where such interests are overridden by your interests or fundamental rights and freedoms.

We may also rely on your consent to process your Personal Data for a specific purpose (art. 6 (1) (a) of GDPR).

Eventually, we may also process your Personal Data as necessary for the performance of a contract or take steps prior to entering into a contract (art. 6 (1) (b) of GDPR) or legal obligation (art. 6 (1) (c) of GDPR).

Managing and responding to your inquiries or requests: We handle and respond to inquiries or requests that you submit through various means, including where you contact us via the website chat function, sign up to download or receive information from us, sign up for a demo to use our services or products or where you exercise your privacy rights, as detailed in this notice.

- *Legal basis*: performance of the contract or taking steps prior to contracting, legitimate interest, performance of a legal obligation

Personalizing our website to improve your browsing experience: We use your information to tailor our website to your preferences, ensuring a more relevant experience. This may include customizing content and optimizing site functionality to meet your needs.

- *Legal basis*: consent, legitimate interest

Marketing or promoting our services and products: We may use your Personal Data to communicate with you directly about our services, products, offers or events that may be of interest to you or publish your testimonials on our website (respecting your marketing preferences).

- *Legal basis*: consent, legitimate interest

Provision of our services and products to you as a User: We use your information to deliver the services and products you, your administrator or your organization has requested. This may include using your Personal Data to enable you to login and access your account, to respond to your inquiries and provide you with customer support, to send you technical or commercial information as part of the services and on the products, to provide you information about your account, including renewals.

- *Legal basis*: legitimate interest

Customizing the services: We use your information to tailor our services according to your interests and needs as a User, making recommendations to

optimize your use of our services and products and directing you to other relevant features.

- *Legal basis*: legitimate interest

Improving our services and products based on usage data: We use your usage data to create new features and functionalities, improve the operation of the products for all Users, fix bugs and troubleshoot product functionality.

- *Legal basis*: legitimate interest

Business analytics: We use your data to infer your geographic location based on your IP address; to track behavior at the aggregate/anonymous level to identify and understand trends in the various interactions with our services and products, and to conduct internal business analysis based on meta-data about usage, feature adoption and forecasting.

- *Legal basis*: legitimate interest

Monitoring and securing our systems: We use your data to monitor and secure our systems when you visit our website or use our services or products. We may do this by creating service logs, which are factual records of system events, to monitor the proper function of systems and diagnostics, to create an auditable record of system events to assist with system security and reliability, and in general to allow us to be informed on what is happening within the systems.

- *Legal basis:* legitimate interest

Preventing abuse and illegal activities: We use your information to detect, prevent and address any forms of abuse or illegal activities on our platform, including through automated systems that screen content for phishing activities, spam and fraud.

- *Legal basis*: legitimate interest, performance of a legal obligation

Maintaining legal records: We use your information to fulfill certain legal obligations, resolve disputes or comply with regulatory requirements. This may include carrying out our obligations and enforcing our rights arising from any

contracts entered into between you and us, responding to legal requests or preventing fraud. If we receive a subpoena or other legal request, we may need to inspect the data we hold to determine how to respond.

- *Legal basis*: performance of a legal obligation, legitimate interest

Evaluating Job Applicants and recruitment: We use your information to evaluate your skills, qualifications and compatibility for a job, conduct necessary background and reference checks, maintain ongoing communication during the recruitment process and improve our hiring process.

- *Legal basis*: legitimate interest, performance of a contract or taking steps prior to contracting

Automated Decision-Making

At Bynder, we want to emphasize that our recruitment process is designed to ensure fairness and transparency. We do not rely solely on automated decision-making methods, which involve making decisions without human involvement, during the recruitment process.

Security Measures

We implement appropriate technical and organisational measures, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of likelihood and severity for your fundamental rights and freedoms, to ensure a level of security appropriate to such risk.

The measures ensure in particular safeguarding the confidentiality, integrity and availability of the Personal Data by implementing policies and procedures governing, among other things, the encryption of data, access control of data, secure development of our products, secure network, technical vulnerability management.

In its dedication to protect (personal) data, Bynder is certified against ISO

27001:2013, ISO 27018:2019 and ISO 22301:2019 and undergoes annual independent audits as a continuous validation of our compliance against those standards.

Amazon Web Services provides our servers and maintains them in high-security controlled environments pursuant to the **AWS Cloud Security policy**.

Do we sell or share your Personal Data?

We do not sell your Personal Data.

We may share your Personal Data for the purpose of performing our legal or contractual obligations (including to comply with applicable laws, a valid court order, lawful request by authorities or other legal process) or supporting our business. We may transfer the data we control, including Personal Data, in the event of a company reorganization, merger, or sale.

When we share your Personal Data with third parties as part of externalizing the Processing of such data on our behalf, we enter into a Data Processing Agreement that ensures the Processor's obligations are complied with and your rights as a Data Subject are protected.

Your Personal Data may be shared with the following types of third parties:

Service Providers

Bynder may engage with third-party service providers who allow for the performance of certain services on behalf of Bynder. The service providers might support multiple functions across the organization such as analytics, application and website development, marketing, and storage (hosting, data backup), customer services and support. To enable the provision of these services, Bynder might need to share your Personal Data with the service provider.

Partners

Bynder may collaborate with third-party partners in joint initiatives that align with Bynder's business goals and objectives. Your Personal Data may be shared with partners for co-branded promotions, joint research and development efforts, and cross-promotional opportunities.

Integrated Apps

You may use certain third party applications in connection with the services offered by Bynder. These integrated apps may collect your data when enabled or used. Bynder has no ownership or control over what the behavior of these apps and what data may collect. Please review the privacy policies of any third party apps that you wish to integrate before enabling.

Social Media Buttons

Our website may include embedded videos or other social media content from third-party providers. While no data is collected initially, accessing this content may result in data being collected by the respective social media platforms.

Legal and Regulatory Authorities

Your Personal Data may be shared with governmental agencies, law enforcement officers or courts only if required by law (including to meet national security security or law enforcement requirements), a valid court order, or to protect the rights of Bynder.

Potential Acquirers or Mergers

Bynder may share your data with a potential buyer or partner in the event of an acquisition or merger.

Do we transfer your Personal Data?

General Transfers

As an international company with Customers and Users worldwide, we may transfer and access Personal Data around the world, including to and from the United States. To comply with applicable law, we maintain strong data protection and privacy controls to protect your Personal Data during cross-border and international transfers, as well as during periods of storage in foreign countries (e.g. EU Standard Contractual Clauses, and binding corporate rules).

We believe that your essential privacy rights are not contingent on your nationality or residency. While applicable law always governs data privacy matters, we intend for this Global Privacy Policy to apply generally to Users and their Personal Data around the world. Nevertheless, privacy law is a constantly changing landscape so we reserve the right to deviate from this Global Privacy Policy where applicable law provides for a different approach.

Transfers to the United States and onward transfers

Bynder's US based entity, Bynder LLC, complies with the EU-U.S. Data Privacy Framework (EU-U.S. DPF), the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF) as set forth by the U.S. Department of Commerce (collectively referred to as "Data Protection Frameworks"). Bynder LLC has certified to the U.S. Department of Commerce that it adheres to the EU-U.S. Data Privacy Framework Principles (EU-U.S. DPF Principles) with regard to the processing of personal data received from the European Union in reliance on the EU-U.S. DPF and from the United Kingdom (and Gibraltar) in reliance on the UK Extension to the EU-U.S. DPF. Bynder LLC has certified to the U.S. Department of Commerce that it adheres to the Swiss-U.S. Data Privacy Framework Principles (Swiss-U.S. DPF Principles) with regard to the processing of personal data received from Switzerland in reliance on the Swiss-U.S. DPF. If there is any conflict between the terms in this privacy policy and the EU-U.S. DPF Principles and/or the Swiss-U.S. DPF Principles, the Principles shall govern. To learn more about the Data Privacy Framework (DPF) program please visit https://www.dataprivacyframework.gov/, for details about

our certification please see our entry on https://www.dataprivacyframework.gov/list.

Under the Data Protection Frameworks, the Federal Trade Commission (FTC) has investigatory and enforcement powers over Bynder LLC. The FTC oversees adherence to the Data Protection Frameworks.

In case of onward transfers to third parties from Bynder LLC, Bynder has certain liability if those third parties do not comply with the Data Protection Frameworks with regards to the data transferred.

Should you have a Data Protection Frameworks-related complaint, please reach out first to privacy@bynder.com. Bynder LLC is committed to resolving complaints for any issues related to your data transferred or processed under Data Protection Frameworks.

Unresolved or unsatisfactorily addressed complaints may also be submitted to the appropriate data protection authority. Bynder LLC is committed to complying with the advice of the panel established by the EU data protection authorities (EU DPAs), the UK Information Commissioner's Office (ICO), Gibraltar Regulatory Authority (GRA) and the Swiss Federal Data Protection and Information Commissioner (FDPIC) with regard to unresolved complaints concerning our handling of personal data received in reliance on the Data Protection Frameworks.

If the complaint is not resolved through either of the above mentioned methods, you may invoke binding arbitration under certain specific conditions which are further described at:
https://www.dataprivacyframework.gov/framework-article/ANNEX-I-introduction.

How long do we retain your Personal Data?

We retain Personal Data for as long as we reasonably consider it to be necessary for the purposes for which it was collected, after which time we will delete the information. The retention factors may be conditioned by statutory obligations and statutory limitations, need to keep evidence of the performance of our own obligations, completion of the specific purposes when we rely on legitimate interests.

In case of a job application, Bynder may request to retain your personal information for an extended period (2 years) for Job Applicants to be considered for future job opportunities.

What are your rights with respect to our Processing of your Personal Data?

If you are resident in the EEA, Switzerland or UK, you have the following data protection rights, in accordance with the applicable statutory provisions:

- **Right to access** your Personal Data at any time.
- **Right to review, change, update** your Personal Data at any time.
- **Right to delete** your Personal Data at any time.
- **Right to revoke consent** to the Processing of your Personal Data at any time. Withdrawing your consent will not affect Processing of your Personal Data conducted in reliance on lawful Processing grounds other than consent.
- **Right to opt out**, at any time, of receiving direct marketing communication we send you by clicking on the unsubscribe link in the emails we send you or by contacting us.
- **Right to object**, on grounds relating to your particular situation, at any time to the Processing of your Personal Data that is based on legitimate interest.
- **Right to restrict** the Processing of your Personal Data.
- **Right to have your data transmitted** to another Controller.
- **Right to submit a complaint** to a data protection authority about our Processing of your Personal Data. For more information, please contact your local data protection authority. Contact details for data protection authorities in the EEA are available here. For UK residents, the ICO can be contacted here.

As most of the information we collect about you may only identify a particular device or browser, the exercise of your rights may require that you provide us with some additional information so that we can identify you individually to allow us to identify your Personal Data being processed and fulfil your request accurately.

California Consumer Privacy Act (CCPA) Supplement

If you are a resident of California, this supplement to the Global Privacy Policy sets out additional rights and information for you.

Many obligations under the CCPA, and the CPRA are addressed in other provisions of the Global Privacy Policy. This Supplement is meant to fill in the gaps for California residents and the terms used in this Supplement are either defined in the Global Privacy Policy or in the text of the CCPA.

Bynder has not sold the personal information of any California residents in the preceding 12 months.

CCPA Consumer Rights

- **The right to access**, and to know both the categories of personal information ,and the specific personal information we collect, the purposes for which personal information is collected, whether personal information is sold or shared, and the retention period for the personal information.
- **The right to have your personal information deleted**, subject to some legal limitations.
- **The right to the correction** of inaccurate personal information.
- **The right to data portability**.
- **The right to limit** the sharing of sensitive personal information.
- **The right to opt-out of automated-decision making**.
- **The right to opt-out of the sale or share** of personal information.
- **The right to request disclosure** of the personal information collected.
- **The right to disclosure** of information disclosed for valuable consideration.

How can you contact us in case of a complaint?

General Requests

You may submit a request to exercise your rights by email to privacy@bynder.com. Please be as specific as possible and detail at least the following:

- The right you wish to exercise or the goal of the request
- Your name
- Your email address.

In the event the email address which we receive the request from and the one the Personal Data belongs to do not match, we may request additional information to verify the identity of the Data Subject.

Submitting Requests under CCPA

California residents may submit requests for information under the CCPA to Bynder by email to **privacy@bynder.com** or by calling our U.S.-based toll-free telephone number: 1 (877) 460-2314.

Please be as specific as possible when you exercise your rights under CCPA and submit a request regarding your personal information.

Policy Updates

This Global Privacy Policy is reviewed on a regular basis and is updated as often as necessary. Any update to this Global Privacy Policy is posted publicly on the Website on this page.

Controllers

Bynder BV
Overtoom 16
1054 HJ Amsterdam
The Netherlands
Attn: Bynder Legal Team – Privacy

or

Bynder LLC
321 Summer Street Suite 100
Boston, MA 02210
Attn: Bynder Legal Team – Privacy

or

Bynder Pty Ltd
Level 7, 180 Flinders Street
Melbourne VIC 3000
Attn: Bynder Legal Team – Privacy

or

Bynder Ltd
3 Waterhouse Square, 138-142
EC1N 2SW London
Attn: Bynder Legal Team - Privacy

or

Bynder Software SL
Carrer de Balmes 7, 5A
08007 Barcelona
Attn: Bynder Legal Team - Privacy

or

Bynder Software FZ-LLC
Shared Desk Unit No. SD2-89
Ground fLoor, Building 7
Dubai Outsource City
P.O. Box 345858 Dubai
Attn: Bynder Legal Team - Privacy.

Contact information of the data protection officer

Blaakhaven kantoorgebouw
Blaak 6,
3011 TA Rotterdam
The Netherlands
Email address: privacy@bynder.com
Phone: +31 (0) 10 899 0800