Bynder Acceptable Use Policy

This Acceptable Use Policy ("AUP") describes acceptable use of and access to any Product offered by Bynder, including any Mobile Apps, whether it is provided directly or through another party. By accessing or using the Products, Customer agrees to the terms of this AUP and will be held responsible for any violations hereof. Without Customer's agreement to abide by this AUP, Bynder cannot provide the Products. Use of the Bynder Products shall be subject to the Bynder Privacy Policy.

Unless otherwise defined herein or in the Agreement between Customer and Bynder, all capitalized terms used within this AUP have the following meaning:

Customer: a company, or its representative, with a current agreement with Bynder for the purchase of Products or a user of a free trial version of Bynder.

Customer Data: all items uploaded to the Products

Intellectual Property Rights: all and any copyright, know-how, rights in inventions, patents, trade secrets, trademarks and trade names, service marks, design rights, rights in get-up, database rights and rights in data, the right to sue for passing off, utility models, domain names, rights in goodwill and all similar or equivalent rights and in each case, whether registered or not, including any application to protect or register such rights and all renewals and extensions of such rights or applications, whether vested, contingent or future, and wherever existing.

Products: Bynder software products and services, including Bynder trial versions, additional products purchased, and any modified, updated or enhanced versions of such products and services that Bynder may make available.

1. Prohibited use and content.

Customer may not upload Customer Data or use the Products in a manner that:

1.1 violates any local, state, national, foreign or international Regulations, including data protection and privacy regulations, or fails to secure all required consents from data subjects;
1.2 advocates or induces illegal activity;
1.3 infringes or misappropriates the Intellectual Property Rights of another party;
1.4 publishes, posts, uploads, or otherwise distributes any software, music, videos, or other material protected by intellectual property laws (or by rights of privacy or publicity), unless Customer has all rights and consents required to do so;
1.5 is threatening, abusive, harassing, stalking or defamatory;
1.6 is deceptive, false, misleading or fraudulent;
1.7 modifies, alters, tampers with, repairs, reverse engineers, disassembles, decompiles or otherwise creates derivative works of any software included in the

Products (except to the extent this is expressly permitted under a separate license agreement for the creation of derivative works);

1.8 is invasive of another's privacy or otherwise violates another's legal rights (such as rights of privacy and publicity);

1.9 involves uploading files that contain viruses, malware, corrupted files, or any other similar software or programs that may damage the operation of another person's computer;

1.10 interferes with or disrupts the Products or servers or networks connected to the Products;

1.11 uses any high volume automated means (including robots, spiders, scripts or similar data gathering or extraction methods) to access the Products or any other accounts, computer systems, or networks connected to the Products (each a "System");

1.12 downloads any file that Customer knows, or reasonably should know, cannot be legally distributed in that way;

1.13 falsifies or deletes any author attributions, legal or proprietary designations, labels of the origin or source of software, or other material contained in a file that is uploaded;

1.14 restricts or inhibits any other Customer from using the Products;

1.15 harvests or otherwise collects information about others, including e-mail addresses, without their consent;

1.16 violates the usage standards or rules of an entity affected by Customer's use, including without limitation any internet service provider (or ISP), ESP, or news or user group (including, for example, circumventing or exceeding equipment use rights and restrictions and/or location and path identification detail); and/or

1.17 is legally actionable between private parties.

2. Customer will use the Products for Customer's internal business purposes and will not violate the security or integrity of a Product in any way, including but not limited to:

2.1 willfully tampering with the security of the Products;

2.2 accessing data on the Products not intended for Customer;

2.3 logging into a server or account on the Products that Customer is not authorized to access;

2.4 attempting to probe, scan, or test the vulnerability of any Products or to breach the security or authentication measures without proper authorization;

2.5 willfully rendering any part of the Products unusable;

2.6 attempting to gain unauthorized access to any portion of the Products whether through hacking, password mining, or any other means;

2.7 monitoring data or traffic on a system without permission;

2.8 leasing, distributing, licensing, selling, or otherwise commercially exploiting the Products or making the Products available to a third party other than as contemplated in the Agreement;

2.9 using the Products for timesharing or service bureau purposes, or otherwise for the benefit of a third party without our prior written consent; and/or

2.10 providing to third parties any evaluation version of the Products without our prior written consent.

3. No SPAM Permitted; Email Opt-Out Requirements

Customer may not use the Products in any way (directly or indirectly) to send, transmit, handle, distribute or deliver:

3.1 unsolicited email ("spam" or "spamming") or commercial electronic messages in violation of the CAN-SPAM Act, Directive 2002/58/EC, or Canada's Anti-Spam Legislation, Dutch Telecommunications Act 1998 ("telecommunicatiewet") or any other applicable laws;

3.2 email to an address obtained via Internet harvesting methods or any surreptitious methods (e.g., scraping or harvesting); or

3.3 email to an address that is incomplete, inaccurate and/or not updated for all applicable opt-out notifications, using best efforts and best practices in the industry.

Customer warrants that Customer will promptly comply with all opt-out, unsubscribe, "do not call", and "do not send" requests from users of Customer's services and recipients of Customer's emails. Customer further warrants that each email Customer sends or which is sent on Customer's behalf using the Products will contain:

3.4 header information that is not false or misleading; and

3.5 an advisement that the recipient may unsubscribe, opt-out or otherwise demand that use of its information for unsolicited, impermissible, and/or inappropriate communication(s) as described in this AUP be stopped, and must clearly indicate how the recipient can notify Customer that it wants to unsubscribe, opt-out, or stop this use of its information.

These requirements may not apply if the email concerned is strictly transactional in nature and/or these requirements are otherwise subject to a legal exception.

4. Prohibited Email Content and Formatting; Email Best Practices

Customer is prohibited from using the Products to send emails to addresses acquired from purchased lists. Emails sent or caused to be sent to or through the Products may not:

4.1 contain false or misleading information or content or use or contain invalid or forged headers or invalid or non-existent domain names;

4.2 employ any technique to otherwise misrepresent, hide, or obscure any information in identifying the point of origin or the transmission path or any other means of deceptive addressing;

4.3 use a third party's internet domain name without their consent, or be relayed from or through a third party's equipment without the third party's permission; and/or

4.4 use Bynder's trademark(s), tagline(s), or logo(s) without our prior written consent and, with such consent, only pursuant to the limits placed on any such use.

5. Bynder Trademark Use

Unless Customer has Bynder's express prior written permission, Customer may not in any way use, remove, or alter any name, logo, tagline, or other mark of Bynder or the Products, or any identifier or tag generated by the Products, including without limitation:

5.1 as a hypertext link to any website or other location (except as provided for or enabled expressly by us); and/or

5.2 to imply identification with Bynder as an employee, contractor, agent, or any other similar representative capacity.

6. Customer Reporting Suspected Violations

Customer can report abuse of this AUP to legal@bynder.com. If Customer is the recipient of email messages sent using the Products that Customer knows or suspects were sent in violation of this AUP, Bynder encourages Customer to report this to Bynder by forwarding an unaltered copy of the received email.

7. Assessing Compliance with the AUP

Bynder has the sole discretion to determine whether Customer Data or Customer's use of the Products is prohibited. All Customer Data that is provided to Bynder or actions that are performed via Customer's account, whether provided or performed by Customer's employees, Customer's contractors, or Customer's customers and end users, are the sole responsibility of Customer.

8. Monitoring and Enforcement

Bynder may:

8.1 investigate violations of this AUP or misuse of the Products;

8.2 take measures to prevent security threats, fraud, or other illegal, malicious, or inappropriate activity;

8.3 notify Customer of violations of this AUP or misuse of the Products, remove any prohibited materials and/or deny access to any person who violates this AUP;

8.4 suspend or terminate use of the Products being used in a way that violates this AUP or any other agreement Customer has with Bynder for the use of the Products;

8.5 use its discretion in developing and implementing mechanisms to enforce this AUP;

8.6 report any Customer activity that it suspects violates any law or regulation to appropriate law enforcement officials, regulators, or other appropriate third parties. Bynder's reporting may include disclosing Customer information, as necessary.

8.7 disclose information regarding Customer's use of any Products to satisfy any law, regulation, government request, court order, subpoena, or other legal process. If Bynder makes this type of required disclosure Bynder will notify Customer, unless Bynder is required to keep the disclosure confidential.

9. Fair Use

We aim to ensure that all of our Customers enjoy fast and reliable service.

9.1 The following traffic prices apply:

Traffic	Price per GB
First 8 TB per month	0.00
More than 8 TB per month	0.15 USD 0.13 EUR 0.11 GBP
More than 350 TB per month	Bynder will contact Customer

9.2 Bynder monitors each Customer's outgoing traffic volume. Any outgoing traffic volume in excess of 8 TB per month ("Additional Traffic") will attract costs as stated in the above schedule.

9.3 Bynder will invoice each Customer for its Additional Traffic, if any, on a monthly. Such invoices are subject to the Payment Terms in the Agreement between Bynder and Customer.

10. Updates to the AUP

Bynder may update and change any part or all of this AUP. If Bynder updates or changes this AUP, the updated AUP will be posted publicly at bynder.com/en/legal. Bynder will notify Customer with an email and a notification in the Bynder Product. The updated AUP will become effective and binding thirty (30) days after it has been posted. When Bynder changes this AUP, the "Updated" date below will be changed to reflect the date of the most recent version ("Update Effective Date"). Bynder encourages Customer to review the online AUP periodically. If Customer objects to any such changes, Customer's sole recourse shall be to cease using the Products. Continued use of the Products following the Update Effective Date of any such changes shall indicate Customer's acknowledgement of such changes and agreement to be bound by the updated AUP.

This AUP was last updated on: 16 August 2016.