GDPR Policy | Backblaze Online Backup

Privacy Notice for EEA/EU Residents (GDPR)

Last updated: July 21, 2023

On July 16, 2020, the Court of Justice of the European Union issued a judgment declaring as invalid the European Commission’s Decision (EU) 2016/1250 of 12 July 2016 on the adequacy of the protection provided by the EU-U.S. Privacy Shield. As a result of that decision, the EU-U.S. Privacy Shield Framework is no longer a valid mechanism to comply with EU data protection requirements when transferring personal data from the European Economic Area (EEA) to the United States. That decision does not relieve participants in the EU-U.S. Privacy Shield of their obligations under the EU-U.S. Privacy Shield Framework.

On September 8, 2020 the Federal Data Protection and Information Commissioner (FDPIC) of Switzerland issued an opinion concluding that the Swiss-U.S. Privacy Shield Framework does not provide an adequate level of protection for data transfers from Switzerland to the United States pursuant to Switzerland’s Federal Act on Data Protection (FADP). As a result of that opinion, organizations wishing to rely on the Swiss-U.S. Privacy Shield to transfer personal data from Switzerland to the United States should seek guidance from the FDPIC or legal counsel. That opinion does not relieve participants in the Swiss-U.S. Privacy Shield of their obligations under the Swiss-U.S. Privacy Shield Framework.

In light of the ruling issued by the Court of Justice of the European Union on the invalidation of the EU-U.S. Privacy Shield, and the opinion provided by the Federal Data Protection and Information Commissioner (FDPIC) of Switzerland on the inadequacy of the Swiss-U.S. Privacy Shield Framework, we are no longer relying on these frameworks when transferring personal information from the EEA and Switzerland to the United States. We continue to comply with applicable EU data transfer requirements, including adherence to no less than the principles of the EU-U.S. and Swiss-U.S. Privacy Shield Frameworks. We are closely monitoring development of international data-transfer mechanisms under the GDPR and will update our policies accordingly.

Despite this, Backblaze complies with the EU-U.S. Privacy Shield Framework and Swiss-U.S. Privacy Shield Framework as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of personal information transferred from the European Union and Switzerland to the United States. Backblaze has certified to the U.S. Department of Commerce that it adheres to the Privacy Shield Principles. If there is any conflict between the terms in this privacy policy and the Privacy Shield Principles, the Privacy Shield Principles shall govern. To learn more about the Privacy Shield program, and to view our certification, please visit
In compliance with the Privacy Shield Principles, Backblaze commits to resolve complaints about our collection or use of your personal information. EU and Swiss individuals with inquiries or complaints regarding our Privacy Shield policy should first contact Backblaze at privacy@backblaze.com.

Backblaze has further committed to refer unresolved Privacy Shield complaints to American Arbitration Association, an alternative dispute resolution provider located at 120 Broadway, 21st Floor in New York, NY 10271 in the United States.

If you do not receive timely acknowledgment of your complaint from us, or if we have not addressed your complaint to your satisfaction, please visit www.adr.org for more information or to file a complaint. The services of the American Arbitration Association are provided at no cost to you.

Inform individuals about (see Privacy Policy FAQs):

- the type or identity of third parties to which your organization discloses personal information, and the purposes for which it does so
- the right of individuals to access their personal data
- the choices and means your organization offers individuals for limiting the use and disclosure of their personal data
- your organization being subject to the investigatory and enforcement powers of the Federal Trade Commission (FTC)
- the possibility, under certain conditions, for the individual to invoke binding arbitration
- the requirement for your organization to disclose personal information in response to lawful requests by public authorities, including to meet national security or law enforcement requirements
- your organization’s liability in cases of onward transfers to third parties

This Privacy Notice is for European Economic Area (EEA) visitors and customers. It supplements the information in our general Privacy Notice, in which we describe how we collect and use your personal data, what we do with the collected data, with whom we share the data, how long we store it and how you can exercise your privacy rights. In this supplemental notice, we provide additional information which is required under European data protection law.

Please also review our Terms of Service and Data Processing Addendum which describe what we can expect from each other when you use our products and services.

Who We Are

Backblaze, Inc. (“Backblaze”) is a US-headquartered data storage provider that offers two
different services:

- **Computer Backup**, which provides unlimited cloud backup for individuals and organizations using Macs or PCs (laptops and desktops); and
- **B2 Cloud Storage**, which provides low-cost cloud storage for individuals and organizations.

Under EU data protection legislation, Backblaze is the controller of processing of personal information described below.

With regard to the processing of files uploaded to our platform by our users when using our Computer Backup and B2 Cloud Storage services, however, Backblaze is the processor and the person or organization contracting with Backblaze is the controller. To learn more about our processing of data as a processor on behalf of a controller, see our [Data Processing Addendum](#).

### Legal Basis for Processing Your Personal Information

Under the European data protection rules, we are required to inform you on which legal basis we do the processing of personal data. Our legal basis for collecting and using the personal information described above will depend on the personal information concerned and the specific context in which we collect it. We will normally collect personal information from you only where we have your consent to do so, where we need the personal information to perform a contract with you, or where the processing is in our legitimate business interests. In some cases, we may also have a legal obligation to collect personal information from you.

If we ask you to provide personal information to comply with a legal requirement or to enter into a contract with you, we will make this clear at the relevant time and advise you whether the provision of your personal information is mandatory or not (as well as of the possible consequences if you do not provide your personal information). Similarly, if we collect and use your personal information in reliance on our legitimate business interests, we will make clear to you at the relevant time what those legitimate business interests are.

If you have questions about or need further information concerning the legal basis on which we collect and use your personal information, please contact us using the contact details provided under the 'How to contact us' heading below.

### Third-Party disclosures and onward transfers

Backblaze shall only disclose the personal data to a third-party on documented instructions from the Customer/Visitor. In addition, the data may only be disclosed to a third party located outside the European Union (in the same country as Backblaze or in another third country, hereinafter “onward transfer”) if the third-party is or agrees to be bound by the Standard Contract Clauses, set out in our [DPA for EEA/ EU Residents](#) or if:

- (i) the onward transfer is to a country benefiting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;
- (ii) the third-party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;
• (iii) the onward transfer is necessary for the establishment, exercise or defense of legal claims in the context of specific administrative, regulatory or judicial proceedings; or
• (iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by Backblaze with all the other safeguards under these Clauses, in particular purpose limitation.

The type of third-parties to which Backblaze discloses and the purposes for disclosure

(a) Backblaze may disclose personal data received under this DPA to third parties, in adherence with the Customer/Visitor’s documented instructions and under the following conditions:

(i) Service Providers: Backblaze may share your personal data with our service providers that perform services on our behalf, such as data analysis, customer service, marketing assistance, information technology support, and related services.

(ii) Affiliates and Partners: Backblaze may share your personal data with our affiliates and partners where it is necessary for providing our services, conducting our operations, or enhancing the user experience.

(iii) Legal and Regulatory Authorities: Backblaze may share your personal data with legal, governmental, or regulatory authorities when required by law or legal process or to establish, protect, or exercise our legal rights or defend against legal claims.

(b) In the case of an onward transfer, the Backblaze ensures that:

(i) the third-party is or agrees to be bound by the Standard Contract Clauses under the appropriate Module set out in our DPA for EEA/ EU Residents

(ii) the onward transfer is to a country benefiting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679;

(iii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679;

(iv) the onward transfer is necessary for the establishment, exercise, or defense of legal claims; or

(v) The onward transfer is necessary to protect the vital interests of the data subject or another natural person.

(c) All disclosures and onward transfers are subject to compliance with all the other safeguards under these Clauses, with an emphasis on purpose limitation.

International Data Transfers

Your personal and non-personal information will be transferred to Backblaze for storage and processing in the U.S.
EU-U.S. and Swiss-U.S. Privacy Shield

When transferring any personal information from the EEA and Switzerland to the U.S., we adhere to the EU-U.S. and Swiss-U.S. Privacy Shield Frameworks, as set forth by the U.S. Department of Commerce. Backblaze has certified adherence to and commits to apply the Privacy Shield Principles to all personal information it processes in reliance on the Shield.

For the purposes of enforcing compliance with the Privacy Shield, we are subject to the investigatory and enforcement authority of the U.S. Federal Trade Commission.

For more information about the Privacy Shield, and to view our certification, see the U.S. Department of Commerce’s Privacy Shield website located at: https://www.privacyshield.gov.

If we have received your personal information in the U.S. and subsequently transfer it to a third-party agent or service provider for processing, and such third-party agent or service provider processes your personal information in a manner inconsistent with the Privacy Shield Principles, we remain responsible under the Privacy Shield unless we can prove we are not responsible for the event giving rise to the damage.

You can direct any questions or complaints about the use or disclosure of your personal information to us at privacy@backblaze.com. We will investigate and resolve any complaints or disputes regarding the use of personal information within forty-five (45) days of receiving your complaint.

We have further committed to using the American Arbitration Association (AAA) to provide an independent recourse method. AAA will handle any complaints Backblaze is unable to resolve.

You may have the option to select binding arbitration for the resolution of your complaint under certain circumstances. To find out more about the Privacy Shield’s binding arbitration scheme please see https://www.privacyshield.gov/article?id=ANNEX-I-introduction.

For information on how to request access, rectification, or deletion of your personal information if it is inaccurate or processed in violation of the Privacy Shield, see the "Your Data Protection and Privacy Rights and Choices" section which follows.

Your Data Protection and Privacy Rights and Choices

If you live in one of the countries of the European Economic Area (EEA), or if you use our service from one of these countries, you have the following rights, which you can exercise at any time as described or by contacting us here:

- If you wish to access your personal information that Backblaze collects. We explain how you can access part of your data through your account here.
- You can correct, update, or request deletion of your details in your Account by logging in to your Account or contacting us.
- You can object to processing of your personal information, ask us to restrict processing of your personal information or request portability of your personal information where applicable and technically possible. You can find more information on objecting to, or
restricting certain processing here. You can find more information on requesting portability here.

- If we have collected and processed your personal information with your consent, then you can **withdraw your consent** at any time. Withdrawing your consent will not affect the lawfulness of any processing we conducted prior to your withdrawal, nor will it affect processing of your personal information conducted in reliance on lawful processing grounds other than consent.

- You have the right to **opt-out of marketing communications** we send you at any time. You can exercise this right here or by using the unsubscribe link provided in each email. It may take up to three business days to remove you from our marketing lists. Please note that even after you opt out, you will still receive Service Emails from us. You can learn more about our Email communications here.

- You have the **right to complain to a data protection authority** about our collection and use of your personal information. Contact details for data protection authorities in the EEA, Switzerland and certain non-European countries (including the U.S. and Canada) are available here.

---

**Obligations of the data importer in case of access by public authorities**

**Notification**

(a) Backblaze agrees to notify the Customer/Visitor and, where possible, the data subject promptly (if necessary with the help of Backblaze) if it:

- (i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

- (ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the Backblaze.

(b) If Backblaze is prohibited from notifying the Customer/Visitor and/or the data subject under the laws of the country of destination, Backblaze agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. Backblaze agrees to document its best efforts in order to be able to demonstrate them on request of the Customer/Visitor.

(c) Where permissible under the laws of the country of destination, Backblaze agrees to provide the Customer/Visitor, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) Backblaze agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.
(e) Paragraphs (a) to (c) are without prejudice to the obligation of Backblaze pursuant to Clause 14(e) and Clause 16 to inform the Customer/Visitor promptly where it is unable to comply with these Clauses.

Review of legality and data minimization

(a) Backblaze agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. Backblaze shall, under the same conditions, pursue possibilities of appeal. When challenging a request, Backblaze shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) Backblaze agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the Customer/Visitor. It shall also make it available to the competent supervisory authority on request.

(c) Backblaze agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

FTC Statement

Backblaze is subject to the investigatory and enforcement powers of the FTC, which is the federal agency responsible for protecting consumers and maintaining competition.

How to Contact Us

DISPUTE RESOLUTION QUESTIONS OR COMPLAINTS?

If you have a question or complaint regarding the covered data, please contact BackBlaze by sending an email to privacy@backblaze.com or by contacting us at:

Privacy Shield organizations must respond within 45 days of receiving a complaint.

If you have not received a timely or satisfactory response from Backblaze to your question or complaint, please contact the independent recourse mechanism listed below:

ICDR/AAA Privacy Shield Program
HR-Related (if applicable)

EU Data Protection Authorities (DPAs): [https://edpb.europa.eu/about-edpb/board/members_en](https://edpb.europa.eu/about-edpb/board/members_en)

Swiss Federal Data Protection and Information Commissioner (FDPIC):

Previous Version(s):

- **October 5, 2020**