

# Privacy Policy

- [Introduction](#)
- [What data is collected?](#)
  - [Self-hosted software tools](#)
  - [Google G Suite](#)
  - [Other legacy and external systems](#)
- [How is the data used?](#)
  - [Email addresses](#)
  - [Full names and personal profile information](#)
  - [Other personal information](#)
- [How is the data shared?](#)
- [How is the data stored?](#)
- [When is the data deleted?](#)
- [Changes to privacy policy](#)
- [Contacting us](#)

## Introduction

The Broadband Forum of 5177 Brandin Court, Fremont, CA 94538, USA (**BBF, We, Us**) is committed to protecting and respecting your privacy.

This policy describes the personal data that we collect, how we use it, how we store it, and when we delete it.

## What data is collected?

### Self-hosted software tools

We host several software tools to support our work. Users sign up for the tools using their full names and corporate email addresses and can then optionally enter personal profile information (photos, phone numbers, social media usernames, website addresses, descriptive text, company name, job title, department and location).

The stored personal data consists of users' full names, corporate email addresses, (optional) personal profile information, and hashed passwords. If requested, personal email addresses are also stored (and are used for communicating with the user).

The tools also store additional information that is necessary for their operation. This data indicates how and when the tools were used by individual users.

The tools maintain log files in order to diagnose and resolve problems. These log files may contain information relating IP addresses to user email addresses.

The tools use "cookies", i.e., information that is placed on your computer or other device when you visit the tools' web sites. These cookies allow you to remain logged into the tools and to move between tools without the need to log in again. You can use browser privacy functions to delete or block cookies, but this may make use of the tools less convenient.

### Google G Suite

We use Google G Suite groups for BBF email lists. Users are subscribed to these groups using their email addresses, and no other personal information is stored.

You may be automatically subscribed to some BBF email lists, e.g., BBF members are automatically subscribed to the "memgen" (all members) list. You can directly manage your subscriptions to other email lists, and you may also be subscribed to other lists appropriate to your role(s) within BBF.

We use Google G Suite calendars for BBF teleconferences. Users are invited to teleconferences using their email addresses, and no other personal information is stored.

Google maintains log files in order to diagnose and resolve problems. These log files may contain information relating IP addresses to user email addresses.

#### Other legacy and external systems

We use other legacy and external systems to store company and user information, manage teleconferences and webinars, handle meeting registrations and payment, manage interactions with individuals and companies who have expressed interest in our work, and send emails on our behalf.

These legacy and external systems include:

- ARO (Association Resources Online) for company and user information
- Authorize.net for processing credit card transactions
- Capsule for customer relationship management
- Constant Contact for managing email communication
- Eventbrite for event management
- Hamilton Group for face-to-face meeting planning
- SendGrid for sending emails to users
- SurveyMonkey for conducting surveys
- Zoom for teleconferencing

In all these systems, users are identified by full name and/or email address (usually corporate email address, but personal email addresses are used if requested).

The following company and user information is stored:

- **Company:** name, URL, address, phone number, signed bylaws, records of dues payments, logos, and general notes regarding contacts and correspondence with those contacts
- **User:** title, first, middle, and last name, email address, company, address, phone numbers, division, manager, contributions submitted, past meeting attendance

Email addresses may be provided directly and voluntarily by individuals who have supplied business cards or signed up for webinars in the expectation that we will store their details. We keep track of the provenance of this information, and we never purchase contact lists from third parties.

We do not usually process or store credit card details (these are supplied directly to a third party payment processor). However, we can receive credit card details, e.g., via secure email, from users who are unable to access the payment processor. In this case the data is deleted immediately after use.

We sometimes receive passport details to be included in visa letters for users who wish to attend our meetings. It can be helpful to retain these details for future use, but we only do this on the explicit request of the passport owner.

We use Google Analytics for tracking usage of our web sites. The data collected is associated with IP addresses, and may contain information relating IP addresses to individual users or households.

Legacy and external systems may maintain log files in order to diagnose and resolve problems. These log files may contain information relating IP addresses to user email addresses.

How is the data used?

#### Email addresses

Email addresses are used to identify users, i.e., as usernames for the various tools. They can be used in several ways:

- To log into a tool
- To identify a user when analyzing tool usage data (any reported results of such analysis will always be anonymized)

Email addresses are also used for contacting users. This can happen in several ways:

- To send an email to a user
- To send an email to a group (email list) of which a user is a member
- To share a piece of content, e.g., a wiki page, with a user or a group of which a user is a member
- To notify a user that some event has occurred, e.g., that a wiki page has been created or updated, or that some software code has been submitted for approval

Full names and personal profile information

We use full names to provide “user-friendly” ways of referring to users, e.g., we might refer to a user as “Edgar Example” rather than as edgar@example.com.

Personal profile information is (optionally) provided by users for use by other users. We don’t rely on this information or make use of it in any way.

Other personal information

As already discussed, we may receive and use credit card details, but we will never store them. Also, we may receive and use passport details, but we will only store them at the explicit request of the owner.

How is the data shared?

Authorized users of our software tools and email lists can view the following personal information:

- Full names, email addresses and (optional) personal profile information for other tools users
- Email list memberships for other tools users (apart from some “closed” lists for which the members are not visible)
- Lists of attendees at all teleconferences (apart from some “closed” teleconferences such as board meetings)

Webinar attendance lists are shared with:

- The third party company that assists with webinar planning

Meeting attendance lists (full names, email addresses and companies) are shared with:

- The hotels that will be hosting the meeting
- The third party company that assists with meeting planning
- The meeting attendees and (via the tools) all tools users

Your personal data will never be made publicly available, will never be shared with any other third parties, and it will certainly never be sold.

How is the data stored?

All personal data is stored on secure servers, and all communication with these servers is encrypted using industry-standard technologies. Passwords are never stored in plain text (only hashed passwords are stored).

Personal data may be transferred to and stored at a destination outside the European Economic Area (EEA) and may be processed by staff operating outside the EEA.

When is the data deleted?

On your request, or if you change employer, or if your employer's relationship with BBF lapses, we will disable your access to all tools and remove you from all BBF email lists.

All messages sent to email lists include information on how to unsubscribe from the list. Requests to unsubscribe from email lists are always dealt with in a timely manner, but note that we will not normally be able to unsubscribe you from lists that are associated with your role(s) within the BBF.

If your tools access is disabled and/or you are removed from an email list, your personal data is hidden from other users but the historical record of your past activities is not deleted:

- Your past tools contributions, e.g., wiki pages or software code submissions, are archived and remain associated with your email address
- Your past email list contributions are (similarly) archived and remain associated with your email address
- Your past meeting attendance is archived and remains associated with your company and email address

In contrast, metadata is subject to a data retention policy as follows:

- Tool usage data is deleted after 6 months
- Tool logs and backups are deleted after 6 months
- Third party metadata (Authorize.net, Google, Capsule, Constant Contact, Eventbrite, Hamilton Group, Meeting Hotels, SendGrid, SurveyMonkey, Zoom) is handled according to the third party's data retention policies
- Any metadata not mentioned above is deleted after 6 months

Note that personal data may persist in stored archives and backups, which will be retained in accordance with our data retention and disaster recovery policies. These backups may persist for an indefinite period of time, but are not available for active data processing.

#### Changes to privacy policy

We review and amend our privacy policy from time to time. The current version of the policy is available at <https://www.broadband-forum.org/privacy>.

#### Contacting us

You have the right to access your personal data. To request access, or to ask any other privacy-related questions, please email [privacy@broadband-forum.org](mailto:privacy@broadband-forum.org). If a request comes from an email address that we don't recognize, we will need to verify your identity.

The BBF data privacy officer and EU representative is William Lupton, [wlupton@broadband-forum.org](mailto:wlupton@broadband-forum.org).