BlueVolt
Knowledge Powers Growth

GDPR Compliance at BlueVolt

What is GDPR?

The General Data Protection Regulation (GDPR), which goes in to effect May 25, 2018, is a new set of laws aimed at enhancing the protection of EU citizens' personal data. The GDPR applies not only to EU-based businesses, but also to any business that controls or processes personal data of EU citizens.

What is personal data?

Personal data is any information that identifies a person directly or indirectly. These include: name, email address, physical address, or even IP address.

> *Art. 4 GDPR: 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person; Source:* https://gdpr-info.eu/art-4-gdpr/

What does this mean to all BlueVolt customers?

As a BlueVolt customer (even those that may not conduct business in the EU), how is what that we are doing to be GDPR compliant affect you?

The GDPR requires increased transparency around data collection and processing. The means users have the right to access and portability, which means users can demand a copy of their data. This builds trust between you and your customers.

The GDPR requires that users have the right to be forgotten. Users can request their accounts be completely deleted. This not only provides them some assurance about the safety of their personal data, it ensures that you have a better view of your active, current learners.

The GDPR requires lawful basis for processing. Essentially, you need a legal reason to use personal data. For example, you have access to user's personal data when the user has expressed *consent* or *legitimate interest*. Making sure lawful basis is established leads to more engaged users.

GDPR Compliance at BlueVolt

Rule	Description	How BlueVolt Addresses	Availability
Lawful basis of processing	You need to have legal reason to access/use your users' data. Those reasons could be: **Consent (opt-in):** User signed up for your public university **Legitimate Interest:** User is an employee or channel partner and has enrolled in a course and/or training track in your university	BlueVolt customers have multiple options to manage users in their university. If the university is public, then users can self-register as a member. If the university is private, users can be created through a third-party integration where the users are managed, or by an administrator manually adding users to the university. In both cases, users are emailed a welcome invitation and a link to log in to access their account.	**Currently Available**
Consent	User needs to be provided "notice" upon initial registration, or log in if already registered, of how their information is processed. The user's consent must also be tracked.	All users upon registration, or upon log in if already a member or made a member via SSO or a User Management Sync with a third-party system, will receive an announcement (customer configurable) that they must agree to. The announcement states that they acknowledge cookies are being used and they accept the privacy policy and Terms of Use, which are linked. This acceptance is tracked and available via an announcement log report.	**Currently Available**
Opt-out of contact	User needs the ability to withdraw their consent to be contacted via email.	All emails sent from the BlueVolt system have an opt-out link provided where the user can indicate that they want all emails via the system to be canceled. *A log will be made available in early June for administrators to view a list of users who have opted out.*	**Currently Available**
Account Deletion	User can request deletion of account/personal identifiable data. Personal data is anything identifiable, such as name and email address.	If using the BlueVolt User Management API, you can perform a GDPR compliant permanent deletion of a user's record via a deletion call through the BlueVolt User Management API. Users may be inactivated individually in the BlueVolt admin portal for customers that manage their users manually. All user accounts are then permanently deleted and are unable to be reactivated on an agreed upon cadence or upon request.	**Currently Available**
Access/Portability	User can request access to the personal data collected about them. Must provide copy of the data in machine-readable format (CSV or XLS).	BlueVolt enables admins to download user's data collected that includes their personal identifiable information and activity history via the Course Enrollment Totals Record report.	**Currently Available**
Modification	User can request to modify their personal data.	Users can modify their information directly in the BlueVolt platform or if the user account if handled via SSO or the User Management integration, the user's information is modified via the 3rd party integrated system and thus automatically updated in the BlueVolt platform.	**Currently Available**
Security Measures	GDPR requires a variety of data protection safeguards, such as encryption at rest and in transit to data obfuscation.	BlueVolt will provide university admins the ability to run a personal data access report that contains a log of admin user ID or API endpoint access, the date and time of access, and the read/write/edit of the personal user data or view of reports that may contain personal user data. *Please contact support@bluevolt.com to have this report generated if needed prior to availability in the admin view of your university.*	In Progress – Available end of June

FAQ

How does BlueVolt use university members personal data? BlueVolt never users their customer's members personal data or shares it with other parties. Your university member's personal data is only available for you to adequately conduct training activities.

Does BlueVolt store university members personal data on testing and development sites? BlueVolt obfuscates personal data on testing and development environments.

What will a log for the purposes of investigation in to data breaches contain? The personal data access log will contain a report of admin user access ID and name, the date and time of access and the read/write/deletion of the personal user data.

If users are managed through an integration with a third-party system, will the user be able to edit their personal data on the BlueVolt platform? No, this information will be read only.

Where is personal data encrypted? User data is stored and encrypted in BlueVolt's instance of Azure Cloud database.

Where and how long are backups stored? Backups are stored on Crash Plan for 2 years. User personal data is obfuscated and back up data is only accessed in case of an emergency roll back for customer account settings. In this case, all user personal data will need to be re-created.