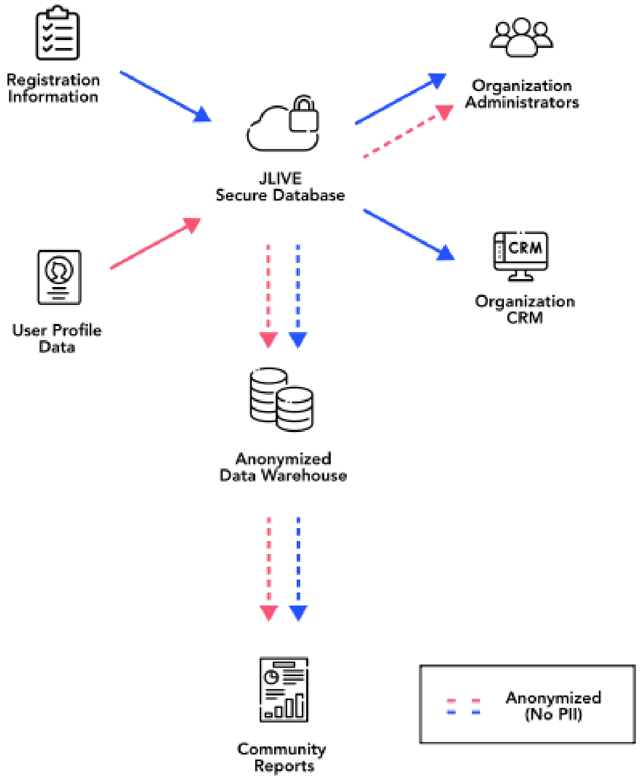
How is data handled?

At Jlive, we take data security and privacy very seriously.

- Data is secured using industry best practices.
- Jlive users can maintain a private User Profile to make registering for events easier.
- Individuals have control over what is shared and with who. For example, when someone registers for an event, the host organization will receive all of the answers they supply when completing their registration form. The host organization will not receive any other personally identifiable information, such as information in stored in their Jlive user profile.
- In addition to receiving event registration form responses, host organizations can view an Event Dashboard that provides useful anonymized demographic information about their registrants. This information will derive from several places including:
  - Registration form information when possible
  - User profile data supplied by the user
  - Anonymized data gathered from prior event registrations by that registrant at any organization on the Jlive platform
- Because Jlive has many orgs using the same platform, Jlive is able to let organizations see the big picture, with respect to data, where other platforms are not.
- Jlive currently integrates with **BBCRM** and has more CRM integrations in the works.
- Jlive APIs make it easy for 3rd parties to build integrations with Jlive if granted approval to do so by Jlive

Flow of Information



Privacy. Transparency. Security.

Event host organizations are only privy to information explicitly shared with them during the event registration process.

Additionally raw JLIVE database data is stripped of personally identifiable information (PII) and stored in a secure and Anonymized Data Warehouse for analysis and trend extraction.

Data & Security

amazon web services

Amazon Data Warehouse

AWS and Redshift trusted by the worlds top businesses and government agencies such as Adobe, Pinterest, and Yelp

stripe

Stripe Payment Processing

Stripe is trusted by companies such as Lyft, Shopify and Salesforce to securely store credit cards and process payments.

tenable

Tenable Cyber Exposure

Tenable can see and predict attacks as well as assess risk of our technology infrastructure.

Penetration Testing

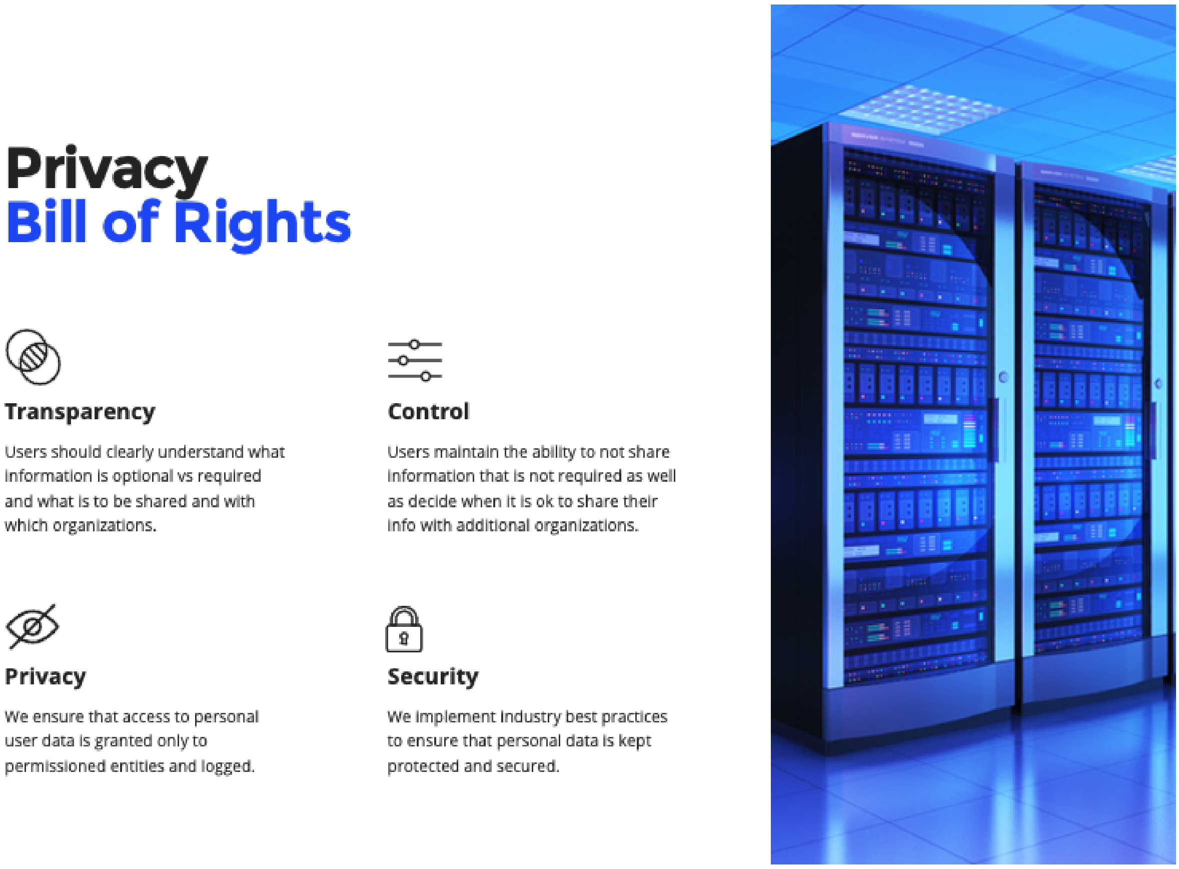
We pay 3rd party experts to hack our systems to discover vulnerabilities

Data Encryption

End to end TLS1.2 encryption in flight and and AES-256 encryption at rest with rotating keys.

Developer Best Practices

Peer reviewed codebase, strong passwords, permissioned data access with logs



Privacy Bill of Rights

Transparency

Users should clearly understand what information is optional vs required and what is to be shared and with which organizations.

Control

Users maintain the ability to not share information that is not required as well as decide when it is ok to share their info with additional organizations.

Privacy

We ensure that access to personal user data is granted only to permissioned entities and logged.

Security

We implement industry best practices to ensure that personal data is kept protected and secured.

Here is the Jlive Privacy Policy.