Overview

In our internal Product Design Principles document for obvi text, the first item reads:

> *#1 - Participant privacy is essential*

With this in mind, we have designed everything from the user interface to the back-end server logging to ensure participants information is not compromised. In addition to participants, we believe our users and have a right to security and privacy.

Participants vs. Users

The entire experience of a Participant is through their own mobile interface. Participants will be given different expectations about how the information they supply will be used by a User. Our goal at obvi is to ensure messages they send are protected in a way that ensures they can only be seen by authorized Project members.

A User conducts projects through the obvi text website. We strive to provide maximum control over these materials while also encouraging best practices.

Privacy by Design

We have made several decisions while building the product to ensure best practices, particularly around PII:

- **obvi does not allow entry of full names**. Anything longer than one word will be shortened to at most first name plus last initial.
- Phone numbers associated with a name will only be shown in the UI until the participant confirms their project invite.
- **Phone numbers are only visible to the Project Owner** (not collaborators)
- **URLs for participant media cannot be shared**. They can only be viewed by authenticated users.
- Views of participant media are logged and trackable to user
- Text responses provided by participants are stored in a database
- Participant text and media is **encrypted at rest**
- To protect data in-transit over the web, “https” is required for all obvi use, as well as all back-end data exchange
- Emails never include participant media

Data Flow & Subprocessors

Data on obvi flows through a number of providers. The privacy and security of each has been carefully considered during product development.

- **Twilio** is the primary interface for Participants to exchange data with obvi text. Their protocols and facilities are based on ISO 27001. gdpr here / whitepaper
- **Heroku** provides our server operations including application servers and databases. Twilio relays data from participants to our application code, on systems operated by heroku. gdpr here
- **Amazon AWS** is the underlying computing infrastructure for Heroku, and also holds all participant media. gdpr here
- **Stripe** is used to handle your credit card payments. We utilize their token-based interface to eliminate storage of PCI data at obvi.
- **Segment** connects our various front-end javascript components to enhance the user experience. It relays browser activity to our web analytics providers. Presently these include: Intercom, FullStory, and Wishpond.
- **Docraptor** will be given transient (<5 minutes) access to participant media when a User requests generation of printed materials.

IT Practices

- All code must be reviewed and approved by a second party
- Code is automatically scanned for vulnerabilities
- 3rd party software libraries are automatically scanned for vulnerabilities as soon as they are known
- No production credentials are held on any staff workstations
- Access to production systems is limited to minimal personnel
- Access logs are reviewed weekly
- Staff access to production systems including application servers, environments, logging, and data-stores is logged.
- Staff is required to use multi-factor authentication and complex passwords for all obvi systems. Passwords are set to expire regularly.
- PII and other sensitive information is not stored in logs
- Database data is encrypted at rest
- AWS holds all participant media in a private S3 buckets which are configured to Block All Public Access. The buckets are encrypted at rest.
- Geographic restrictions are presently in place to disallow non-US based viewing of participant media.

Data Retention

- Data deleted by users is immediately removed from our servers, including 3rd party storage provider AWS.