Crossbar.io Fabric Alpha Test
Data Handling and Privacy Rules

1. Data is Core

Data is at the core of your life, your business - and ours. Access to data has implications in fields such as privacy, security and business secrets. The collection, storage, processing and transmission of data, and keeping these secure, is a complex issue, and we are aware of these complexities.

Our core goal is to handle data in a way which protects you and your interests while allowing us to provide you with our products and services as well as improving these.

The Alpha Test is specifically intended to give us a maximum amount of data which we can use to improve the Crossbar.io Fabric Center service and our software.

In this document we lay out the types of data that we may collect as well as the scope of the collection, storage, processing and transmission.

2. Data Collected

During the Alpha Test period we may collect everything you do via the service if we consider it useful.

Everything here means the data transmitted to the Crossbar.io Fabric Center service when a Crossbar.io Fabric node connects, as well as any data resulting from your interactions with the service, including any responses or events generated by Crossbar.io Fabric nodes based on such interaction.

Everything does not include application data unless you use the tracing API interface, which leads such application data to be transmitted to the Crossbar.io Fabric Center service.

We will notify you should we deviate from these rules for data collection.

While we may collect everything, there are strict limits to what we will do with the collected information.

3. What happens with your data?

3.1. Storage

We store all data as long as necessary to fulfill the purpose for which it was required or which it subsequently serves.

3.2. Processing

In addition to processing data for its immediate purpose (e.g. monitoring, resolving support requests), we run analytics to support the development and improvement of our products and services.

Such processing may e.g. show us how often a particular software feature is being used or where hot spots in the software are.

3.3. Third Parties

We may use third parties as part of our handling of data. We do try to minimize such usage, and will ensure that your data is not handled by any third parties which are not bound by strict privacy regulations.

We will never sell or otherwise hand over your raw data to third parties (except where required to do so by law).

We may sell or pass on aggregate data where the form of such data ensures that no inferences can be made about individual users. We are aware of the problems of pseudonymizing and anonymizing raw data and will never pass on pseudonymized or anonymized raw data.

4. Personal Data

Some data, such as the necessary data to identify you as a user, is personal data, i.e. relates to an identifiable individual. During monitoring and support, other personal data may be transmitted to us or be made accessible to us. As a user, you warrant that you have the necessary rights for transmitting such data to us or granting us access to it. You indemnify us against any claims from third parties with respect to such personal (or indeed other) data for which you do not have the necessary legal rights and which you transmit to us or give us access to.

5. Technical Security Measures

Security is a process, not an outcome. We take this process seriously. We follow current best practices for securing the collection, storage and processing of your data. This means encryption in flight and at rest wherever possible, using up-to-date encryption standards. We closely follow security news and always update software in a timely fashion. To us security is a part of everything, not an afterthought.

Despite the care we take in security matters, security can never be perfect. You agree to not hold us liable for any damages from data leakages which may occur based not on negligence on our part, but on security issues (such as 0-day exploits) which were indefensible at the time of the breach or where a possible defense was not yet part of best practices.