# Data Protection and Privacy on the Emojot Platform

http://help.emojot.com/help/2019/09/29/data-protection-and-privacy-on-the-emojot-platform/

**Last Updated: May 2020**

The Emojot platform plays a role as a **data controller** of its own data and as a **data processor** of customer data. Emojot has adopted the EU GDPR definitions (Article 4), which specifies that a **data controller** is an entity (person, organization, etc.) that determines the why and the how for processing personal data and a **data processor** is an entity that actually performs the **data** processing on the **controller's** behalf.

**Personally identifiable information** (PII) is any data that can be used to identify a specific individual. Social Security numbers or National Identity Card numbers, mailing or email addresses, and phone numbers are commonly been considered PII, but PII can also include an IP address, login IDs, social media posts, or digital images. Geolocation, biometric, and behavioural data can also be classified as PII. The Emojot platform collects and stores **PII data** as a **data processor** and a **data controller**.

Emojot actively ensures compliance as closely as possible with applicable data privacy laws both as a **data controller** of its own data and as a **data processor** of our customers' data. To find out more about the extent of compliance with any particular data protection/privacy regulation or act, please send an email to security@emojot.com.

As a **data processor**, Emojot enables our customers to be compliant as closely as possible with applicable data privacy laws as well. As our customer, if you have any additional questions, please contact your Account Manager.

## Data Privacy: PII Data Subject Requests

As a survey platform, Emojot collects data on survey respondents on behalf of our customers. Generally, individuals have the following rights in relation to their personal data:

- The right to access personal data.
- The right to rectify inaccurate personal data.
- The right to erase personal data.
- The right to restrict the processing of personal data.
- The right to data portability.
- The right to object to the processing of personal data.
- The right to withdraw consent to the processing of personal data

However, these rights are subject to the scenarios and laws under which certain campaigns are conducted by Emojot's customers, who are the data controllers. If a survey respondent wishes to exercise rights in relation to personal data or personal information that may have been collected via the Emojot platform, the respondent should contact the customer (the data controller) who collected the relevant data.

If an individual wants to exercise their rights in relation to data for which Emojot acts as a data controller, they should contact security@emojot.com.

## Data Privacy: Automated Actions and Profiling

As data controllers, Emojot's customers determine the following about the data stored in the Emojot platform:

- What type of data to collect.
- Who to collect data from.
- Where to collect data.
- What the purpose of the data collection is.
- When to delete data.

Emojot customers must determine whether they have a legal basis for performing automated decision-making and profiling and, if so, whether their performance of such activities complies with applicable laws.

The Emojot platform has the capabilities to allow each of our customers to deal with the data subject requests they receive. Emojot can support any requests made by data subjects via our customers (the data controllers), objecting to automated decision making and profiling.

## Data Privacy: Explicit Consent

Following the EU GDPR requirements, Emojot can obtain consent from survey respondents as a freely given, clear affirmative act. The consent wording can be made clear and concise as the first question in a survey. Following the EU GDPR guidelines, the Emojot platform has the necessary governance capabilities to demonstrate that the data subject has given consent to the processing operation.

Health data is deemed ‘special data’ under GDPR guidelines. Emojot does not directly deal with health data and therefore, has not implemented the more stringent version of the consent used for personal, non-health data.

## Data Protection: Data Encryption

All Emojot data is encrypted at rest and in transit. That means, all the data is encrypted in the database, and the data transfer channels are also encrypted.

## Data Protection: Data Storage

Emojot data is stored in an industry-standard database as a service cloud platform that inherently supports high availability, failovers, and replication. By default, Emojot is compliant with all the infrastructure-related regulatory compliance standards that are associated with our cloud provider (AWS).

## Data Protection: Customer Identity Access Management

All Emojot data stores can only be accessed by applications that are within an isolated private network of AWS and cannot be accessed by any unauthorized entity even if they were able to steal login credentials or data access endpoints to Emojot data stores.

Within the Application level, data access is enabled only via API calls. API call authentication, authorization, and governance are managed and done on various levels by an API Manager. Application-level data access is governed by three layers of access. Account-level, Role-level, and User-level. This management is done using SAML and OAuth2 authorization management protocols. All the customer login credentials are encrypted and are stored in an industry-standard user store. All customer identity management is done by an Identity Server. The Emojot customer accounts' (the data controllers') administrators decide which users should be granted access to PII data. All other customer account users do not have access to PII data.

## Data Protection: Security Monitoring and Governance

Emojot has a continuous process of strengthening, monitoring, and securing the Emojot Platform related services with robust internal protocols and processes. These actions include automated server patching, vulnerability scanning, and continuously reviewing the security of the Emojot platform across the multiple levels of infrastructure, applications, and code, in alignment with the best practices of the IT security industry.

## Data Protection: Data Breaches

The EU GDPR compliance requires that companies report data breaches within a 72-hour window. The Emojot platform governance processes enable us to inform our customers of certain types of data breaches within the 72-hour timeframe, enabling our customers to comply with the GDPR guidelines to a certain extent. Emojot is working on becoming compliant for all types of data breaches.

---