EINS

Third Parties

16/07/2020

Controller details

Controller of the EINS App in Liechtenstein is the Global Citizen Foundation, a non-profit organization registered in 9495 Triesen, Landstrasse 40, Liechtenstein.

Register number: FL-000.2.603.048-9

Development

The EINS App is developed by Via AG registered in 9495 Triesen, Landstrasse 40, Liechtenstein.

Register number: FL-0002.617.997-2

Third-Party Overview

Overview of all third parties involved in data processing or providing tech services.

External Data Processing Services

Name	Legal Company	Company address	Location	Data Processing Agreement	Contracting Party
Sentry	Functional software Inc.	132 Hawthorne St, San Francisco, CA 94107, United States	Google Cloud (unclear)	https://sentry.io/legal/dpa/1.0.0/	VIA
AWS	AWS EMEA SARL	38 avenue John F. Kennedy, Luxembourg, L-1855, Luxembourg	Europe	https://aws.amazon.com/agreement/	VIA

EINS
By GCF

Other Services

Name	Legal Company	Company Address	Location	Data Processing Agreement	Contracting Party
Firebase	Firebase Inc.	1600 Amphitheatre Pkwy, Mountain View, CA 94043, US	Europe	https://cloud.google.com/terms/data-processing-terms	VIA
Github	GitHub Inc.	88 Colin P Kelly Jr Street San Francisco, CA 94107 United States	Mostly US	NA - No data access/storage/relevance, only used for source control	VIA
Big Query	Google LLC	Gordon House, Barrow St, Dublin, D04 E5W5, Ireland	Can select Europe	NA - No data access/storage/relevance https://cloud.google.com/terms/data-processing-terms	VIA
Crashlytics	Crashlytics Inc.	One Kendall Square B3201, Cambridge, MA, 02139, USA	Europe	https://firebase.google.com/terms/crashlytics-app-distribution-data-processing-terms	VIA

Note that Google Big Query at no point has access to any EINS or EINS user data. It is simply used to retrieve statistical information on the number of current cases both globally and on a country by country basis.

Data Sensitivity

This section defines data sensitivity according to GDPR, before breaking down what data the EINS application handles into the categories outlined and then finally analyses what third party services have access to this information.

Definition of Sensitivity

GDPR defines data sensitivity as any information relating to an identified or identifiable natural person. It can be broken up into the following categories:

- **Restrictive Data:** this is data which if exposed poses the largest risk to the organization and must be kept secure
- **High Risk:** this is data which if exposed, could cause harm to the business and individuals
- **Medium Risk:** this is data which if exposed, could cause limited harm to individuals and the business
- **Low Risk:** Public information, which if exposed would not cause any harm to the individual or business.

Definition of EINS Data

See the table below for all the data that EINS handles, alongside its categories and what third-party service has access to it.

Data Point	Category	Sensitivity	Storage location	Third-Party Access
App Instance Id	App Instantiation	Low	Device	Firebase
Hashed App instance Id	Registration	Low	Device, server	
Device Private Key	Registration	Restrictive	Device	
Device Public Key	Registration	Low	Device, Server	

Country	Registration	Low	Device, server	
Language	Registration	Low	Device, server	
Device Operating System	Registration	Low	Device, server	
Push Token	Registration	Medium	Device, Server	Firebase
Age (16 or over)	Registration	Medium	Device	
COVID Status	Survey	High	Device, (optional)server	
Date of Submission	Survey	Low	Device, server	
Age of User	Survey	Medium	(optional) device, (optional) server	
Test Dates (positive and negative)	Survey	Medium	(optional) device, (optional) server	
Start date of symptoms	Survey	Low	(optional) device, (optional) server	
Symptoms	Survey	Low	(optional) device, (optional) server	
Device Ephemeral Id	Contact tracing	Low	Device, server (conditional), other devices	Publicly broadcast and available

EINS
By GCF

Received Ephemeral Id	Contact tracing	Low	Device	
Day of Contact	Contact tracing	Medium	Device	
Exposure Measurement	Contact tracing	Medium	Device	
Source Code		Low	Cloud	AWS, Github, Publicly available

***note:** for all cells left blank above there is no third-party access

Sensitive Data Mitigation

See below for areas in which sensitive data undergoes processes to protect it:

- **Survey Data:** All user information in the survey is fully optional, on top of this the user can choose to share this information with the server or not.
- **COVID Status:** This information is stored on the server independently of any identifying information meaning it is completely anonymous.
- **Date Of Submission (Survey):** On the server, this is stored separately from the actual survey data. It is only stored against the hashed app instance Id for validation purposes
- **Age (survey)**: The age is 'fuzzed' by adding +-2 years to the age randomly when it is submitted to the server.

Third-Party Data Considerations

This part of the document analyses all instances in which third-party services have access to an EINS user's data, and the steps that EINS takes to mitigate this risk.

How (US) service providers are kept out of core functionalities:

Service Provider access is controlled via policy systems, which provide any third party providers with the minimum amount of required access control to areas of the system, by only providing

EINS
By GCF

the specified access needed for that service and or system, as to avoid outright access to core functionalities. It's important to note, no third party has direct access or has access to core functionality to the platform's core systems.

Exposure Notification Considerations

Should a user need to be notified that they have been in close contact with a contagious individual, this notification will be handled on the device between the DP-3T SDK and the EINS application itself. Firebase Cloud Messenger plays no part in this process and therefore will never be able to process the user's information.

EINS
By GCF