Fortanix®

Case Study

# University of Groningen achieves data sovereignty and European data compliance with Fortanix for Google Cloud Platform

university of groningen

behapp

## Customer Profile

Founded in 1614, University of Groningen is the second oldest university in Netherlands with a reputation of excellence in academic research and ranked as a top 100 institution in the global Shanghai ranking. With more than 30,000 students today, it powers some of the most transformative breakthroughs in research activities.

## About Behapp project

The Behapp project offers a fully managed digital phenotyping platform as a service. Digital phenotyping is the measurement of human behavioral phenotypes using personal devices, and is rapidly gaining traction in the field of research into mental / brain disease and more.

Incubated at the Faculty of Science and Engineering, University of Groningen, Behapp is first-and-foremost a research instrument for use in formal (medical) scientific research contexts. Behapp specializes in the collection of smartphone-based data that is descriptive of people's social behavior in terms of mobility and communication. Learn more about the Behapp Project here

> We believe that nowadays much of our behavior in terms of daily social functioning is captured by the smartphones that we carry with us. Knowing that social behavior and mental / brain disease are closely related, we started developing Behapp for the study of these diseases. We think that smartphones, and subsequently smartphone-based behavioral data, could be a valuable proxy for daily social functioning and thus help further our knowledge of mental and brain disease in general.

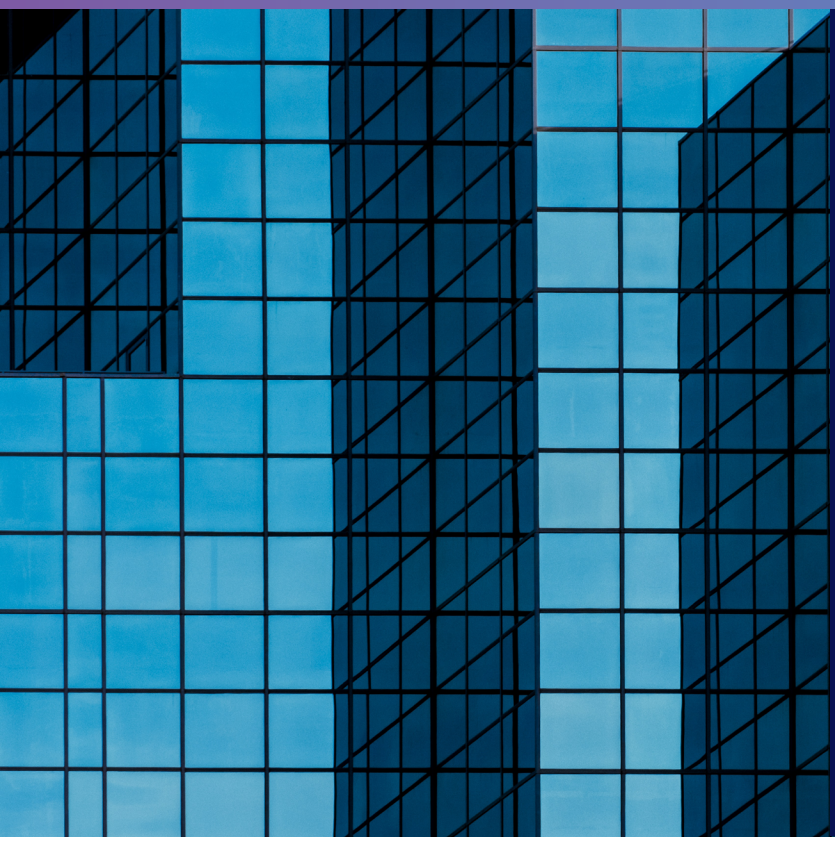
**RAJ JAGESAR,** Project Lead, Behapp Research Program

## Business challenge

For Raj and his colleagues, what started off as a project with a humble and simple IT infrastructure quickly ramped up to involve multiple European multi-center studies resulting in high volume data ingestion rates. Some of this data was directly identifiable given the need to study one's mobility through the collection of location data and required extensive measures to safeguard the privacy of participants. Combined with the GDPR coming in effect, and ethical review boards increasingly becoming aware of the privacy implications of such technology driven research initiatives, the team needed an ironclad data security and privacy strategy.

## What were they looking for? - Key requirements

With all of the data being hosted on Google Cloud Platform (GCP), the team relied on the cloud-native encryption and the Key Management Service (KMS) offered by Google. While this offers a good measure of data security, Raj and his team were seeking greater control over the keys. To gain stronger control over key use and guarantee transparency, it was imperative to involve an independent third party as key manager.



> Google had its own Key Management Service which works great and helped us tremendously in closing our encryption hierarchy. But from a European perspective, given the enactment of the U.S. Cloud Act in 2018 and the termination of the EU-US Privacy Shield we knew that fully relying on Google alone for encryption services would pose a privacy risk towards our research participants.

**RAJ JAGESAR,**
Project Lead, Behapp Research Program

The team operated with limited resources and benefitted greatly from various serverless technologies offered by Google Cloud Platform, enabling a high level of technical maturity in terms of robustness, scalability and security. They preferred to keep this infrastructure in place but needed to get an additional layer of encryption isolating the data from U.S. government data subpoenas.

Compliance regulations like GDPR and Schrems II require organizations to have the ability to revoke access to data at any time and store the encryption keys outside the cloud as additional data protection measures. This prompted the project team to look for a trusted and independent third-party vendor who could help complete this security hierarchy – one final lock that could give them full control over the encrypted cloud data. This also meant that the solution had to seamlessly integrate with Google Cloud services that the project was operating on.

## The Fortanix Solution- Protecting the keys to the kingdom

Fortanix Data Security Manager (DSM) platform was deployed as a Service (SaaS) with integrated hardware security module (HSM), key management, encryption, shared secrets management, and tokenization capabilities. Fortanix seamlessly integrated with Google Cloud Platform's (GCP) External Key Manager service that enabled customers to move the data to the cloud and get the same level of security for keys that they are used to in their own on-premises environments. Encryption keys are never stored on GCP. They are always under customer control, away from the cloud. At a click of a button, in real time, it was possible to enable and disable access to data from specific instances and locations.

### Easy to use and DevOps friendly solution

The cloud agnostic solution is DevOps/SecOps friendly, easy to use, and enables customers to centrally implement and manage multiple data security capabilities from a single console.

### End-to-end security

for keys and data (at-rest, in-transit, and in-use) protected with layers of defense including Confidential Computing, powered on Intel® SGX, and FIPS 140-2 L3 certified Hardware Security Modules (HSMs); Only authorized users can access keys.

### Highly scalable and available service

Scales horizontally and geographically as demand for managing keys and secrets increases. Solution provided automated load balancing, fault-tolerance, disaster recovery, and high availability. Service is globally available with multi-region deployment.

## 'As Is Configuration'


- Keys are held within Google Cloud
- Customers need to trust Google Cloud
- Option to store keys in Google Cloud HSM
- Most of the compliance not met

## With Fortanix Data Security Manager


- No need to trust external party with sensitive data
- Master key remains under sole control of customer within Fortanix FIPS 140-2 Level 3 HSM
- Meets highest compliance requirements
- Improved security posture

## Why did they choose Fortanix?

After a thorough evaluation of multiple vendors, the team chose Fortanix for its advanced data security capabilities and seamless integration with Google Cloud Platform.

> We were looking for a vendor selected by Google Cloud as a trusted provider of encryption services that could integrate directly with Google Cloud Platform", said Raj Jagesar. He further points out: "Fortanix met this criterion and its solution stood out with the most mature operational dashboard for independent management of keys", Raj continues: "Equally as mature was the application programming interface (API) of the solution which enabled us to integrate and deploy Fortanix SaaS DSM in less than a week.

**RAJ JAGESAR,** Project Lead, Behapp Research Program

### What made the Fortanix solution unique:

- Ease of deployment, integration, and management
- Mature and well documented API
- Excellent pre- / post- sales support and onboarding

## The Impact

The project team was able to get the solution up and running in days, with minimal impact on the day-to-day research activities, through which Fortanix helped create a solid data security and privacy strategy.

### Enabling data sovereignty

With Fortanix for Google Cloud Platform, it was possible for the customer to exercise much greater control over their keys, mitigate the risk of uncontrolled data access, and ensure regulatory compliance in the EU.

### Documenting compliance

It was important to furnish documents for ethical reviews and reinforce the robust security and privacy narrative of this project. The transparent security architecture, simplified auditing and logging capabilities which has helped the Behapp team to furnish the necessary documentation on the data privacy controls being implemented. This has allowed the team to move through ethical reviews with confidence and speed.

> Given the current state of data access and retention laws in the U.S. and privacy laws in the E.U. it is difficult for European initiatives to make use of services from U.S. cloud vendors. Your data needs to be sovereign, as in handled in a way to circumvent the U.S. Cloud-Act. But at the same time, you are at a significant disadvantage if you are unable to use services of large American cloud vendors such as Google due to a lack of comparable alternatives in the European tech space. Fortanix enables us to use Google in a responsible way while meeting compliance requirements such as GDPR and Schrems II.

**RAJ JAGESAR,**
Project Lead, Behapp Research Program

FORTANIX DATA SECURITY MANAGER

FORTANIX FOR GOOGLE EXTERNAL KEY MANAGER