superevent

Superevent BV
John M. Keynesplein 36
1036 KP Amsterdam
Netherlands

PO Box 75643
1118 ZR Amsterdam
The Netherlands

+31 20 206 1990
info@superevent.com
superevent.com

Superevent data security

Last updated on 31 January 2019

Superevent has security and your data as its highest priority. We have taken significant measures to protect it, through both technical and procedural processes. If you have any questions after reading this document, please let us know. We will never share your data with any third parties, nor use your data for any other purpose than your event app.

Hosting

Superevent is hosted in the EU on Amazon AWS, the leading cloud provider. AWS's data centers are state of the art, utilizing innovative architectural and engineering approaches. AWS data centers are housed in nondescript facilities. Physical access is strictly controlled both at the perimeter and at building ingress points by professional security staff utilizing video surveillance, intrusion detection systems, and other electronic means. Authorized staff must pass two-factor authentication a minimum of two times to access data center floors.

Encryption

Superevent uses bank-grade TLS AES 256 encrypted connections with strong protocols to transfer data from and to the Superevent platform. All data is encrypted at rest.

Software

The software and applications of Superevent are architected, designed and developed according to industry best practices. Measures are in place to prevent vulnerabilities within the software, unauthorized access and user-input is always validated.

24/7 Monitoring and testing

Extensive performance and availability monitoring allow us to keep a close eye on system health and mitigate unforeseen issues early on. Continuous automated and manual testing lets us detect potential issues early on.

Data Redundancy

Our main databases run in two different datacenters replicated as high availability solution. A third replicated database server runs in a different geographic region as real-time backup. All servers are physically backed up every five minutes within their cloud provider's region. Every 30 minutes a logical backup is taken and stored at a different cloud provider in three geographical regions. All customer data stays within the EU.