Security Policy

Security is a top priority for Azopio and to deliver the highest standard of protection we put in place a security policy leveraging the expertise and experience of our partners whilst implementing ultra-secured technologies and frameworks:

- Our Technical infrastructure is fully redundant and hosted by OVH in France;
- All data transfer is SSL secured;
- Azopio and its partners is PCI-DSS (Payment Card Industry Data Security Standard) level 1 compliant;

1. Highest security standard of our technical infrastructure through OVH

High security datacenters:

All access to the OVH premises is strictly monitored. To prevent any intrusions or hazards, every boundary is secured using barbed-wire fencing. Video surveillance and movement detection systems are also in continuous operation. Activity within the datacentres and outside the buildings is monitored and recorded on secure servers, while the surveillance teams are on site 24/7.
In order to control and monitor access to the OVH premises, strict security procedures have been put in place. Every member of OVH staff receives a RFID name badge which is also used to restrict their access. OVH employee access rights are reassessed regularly, according to their remit. To access the premises, OVH employees must hand in their badges for verification, before passing through the security doors.

Fire risk management:

Every datacentre room is fitted with a fire detection and extinguishing system, as well as fire doors. OVH complies with the APSAD R4 rule for the installation of mobile and portable extinguishers, and also has the N4 conformity certification for all their datacentres.

Network security:

OVH deploys its fibre optic network across the globe and its technology is installed and maintained by in-house teams of engineers.
OVH has also chosen to build its network in a totally redundant manner - multiple security measures have been put in place, so as to eliminate any risk of failure.

Server security:

The OVH teams provide a human presence in the datacentres 24 hours a day and 365 days a year, to guarantee that the servers are constantly maintained.

Electrical supply:

The OVH datacentres are powered by two separate electrical power supplies and are also equipped with UPS devices. Power generators have an initial autonomy of 48hrs to counteract any failure of the electricity supply network.

Anti-DDoS protection:

All OVH dedicated hosting services include protection against all types of DDoS attacks.

2. All data transfer is SSL secured

SSL (Secure Sockets Layer) is the standard security technology for establishing an encrypted link between a web server and a browser. This link ensures that all data passed between the web server and browsers remain private and integral. SSL is an industry standard and is used by millions of websites in the protection of their online transactions with their customers.

3. PCI compliant and implementation of PCI best practices

Azopio has implemented the following PCI best practices:

- Cardholder data is never being sent without SSL;
- We never log or store any sensitive credit card data (full credit card number or verification value (CVV/CVC));
- We protect our customers by keeping our site safe from cross-site scripting attacks;