mooncare

gammadia(SA)

Our security practices

We are committed to being a trusted partner for our clients. Security is therefore a key concern for gammadia SA.

All of gammadia's software is SaaS (software as a service), which allows us to take charge of the aspects of data security and availability relating to application usage.

1. Legal compliance

As a provider of applications for its clients, gammadia acts as a sub-contractor within the meaning of the Swiss Data Protection Law (LPD). gammadia strictly undertakes to respect its obligations under this law, and, in the interests of transparency, provides an explanation here of the organisational and technical security measures it has implemented. gammadia SA precisely describes the nature of the processing provided as a sub-contractor in its "Agreement on the processing of personal data", which is available on its website.

2. Development and hosting in Switzerland

gammadia uses its own developers to develop its applications in Switzerland. Thesolutions, as well as the personal data they contain, are hosted in data centres run by service providers certified to ISO 27001, all of which are based in Switzerland or in Europe.

3. Data security

We use the protocol TLS to encrypt data in transit. Static data, user IDs and backups are also encrypted using adapted technologies and kept up to date at alltimes.

4. Confidentiality

The data is strictly compartmentalised in order to ensure each client's data is handled confidentially. The architecture of our applications guarantees that the data is safeguarded using dedicated databases and specific perimeters. No information is transferred or divulged to third parties without the explicit consent of the client.

Our employees are contractually obliged to maintain professional secrecy.

5. Availability

All elements of our infrastructure are safeguarded against outages thanks to our equipment redundancy. Our services are monitored 24 hours a day, 365 days a year by our support team. All alerts are dealt with immediately, whether day or night.

Our recovery procedures enable us to rapidly restore service in the event of a major incident.

6. Access control

Client access to applications is protected using a combination of username and password. We are in the process of gradually implementing two-factor authentication (2FA) on our various applications.

Applications developed by gammadia allow users to precisely define which data can be accessed or not by each user. It is the client's responsibility to define their policy for managing passwords, to ensure it is applied properly and to adequately configure the authorisations for its own users.

The various gammadia systems are systematically protected by two-factor authentication. The principle of least privilege is also applied in order to restrict

access.

7. Backups

In order to mitigate the risk of losing data, the databases for our applications are fully backed up every hour and the restoration procedure is tested regularly.

The backups are stored on different sites and are kept in compliance with our retention policy.

8. System updates

Our systems are updated on an ongoing basis. Generally speaking, the redundancy of our systems and our procedures allow us to perform maintenance operations without interrupting our service. Prior notifications are sent to our clients by email in the event that it is not possible to avoid system shut-down.

9. Internal organisation

gammadia has defined its security policies and procedures, and these are communicated to all staff. Employees are trained in cybersecurity when they join the company and are regularly made aware of good practice to be observed in this area.

The IT security officer reports directly to the board of management. A data protection advisor is also appointed

10. Responsibilities

In accordance with legal requirements relating to data protection, gammadia maintains a record of its processing actvities and a record of security incidents.

The principles of data protection by design and by default are applied for all new products developed. Privacy impact assessments are also carried out if the situation requires it.