English version below / Deutsche Version unten

Nos pratiques de sécurité

Nous avons à cœur d'être un partenaire de confiance pour nos clients. La sécurité est donc un thème fondamental pour Gammadia SA.

Tous les logiciels de Gammadia sont de type SaaS (software as a service), nous prenons ainsi en charge les aspects de sécurisation des données et de disponibilité relatifs à l'usage des applications.

1. Conformité légale

En sa qualité de fournisseur d'applications pour ses clients, Gammadia endosse un rôle de sous-traitant au sens de la Loi sur la Protection des Données (LPD). Gammadia s'engage résolument à respecter les exigences qui lui incombent en vertu de cette loi et, dans une démarche de transparence, explique ici les mesures de sécurité organisationnelles et techniques mises en place. Gammadia SA décrit précisément la nature du traitement effectué en qualité de sous-traitant dans son "Accord relatif au traitement des données personnelles" disponible sur son site internet.

2. Développement et hébergement en Suisse

Gammadia développe ses applications avec ses propres développeurs en Suisse. Les solutions, ainsi que les données personnelles qu'elles contiennent, sont hébergées dans des datacenters de prestataires certifiés ISO 27001, tous basés en Suisse ou en Europe.

3. Sécurité des données

Nous chiffrons les données en transit au moyen du protocole TLS. Les données statiques, les identifiants des utilisateurs ainsi que les sauvegardes sont également chiffrés au moyen de technologies adaptées et constamment tenues à jour.

4. Confidentialité

Les données sont strictement compartimentées afin d'assurer un traitement confidentiel des informations de chaque client. L'architecture de nos applications garantit l'étanchéité des données au moyen de bases de données dédiées et de périmètres spécifiques. Aucune transmission ou divulgation d'information n'est faite envers des tiers sans l'accord explicite du client.

Nos employés sont contractuellement soumis au secret professionnel.

5. Disponibilité

Tous les éléments de notre infrastructure sont résilients aux pannes grâce à la redondance de nos équipements. Les services sont monitorés 24h/24h, 365 jours/an par notre équipe de support. Les remontées d'alertes sont traitées immédiatement, de jour comme de nuit.

Nos procédures de reprise en cas d'incident permettent une restauration rapide des services en cas d'incident majeur.

6. Contrôle des accès

Les accès des clients aux applications sont protégés par la combinaison du nom de l'utilisateur et de son mot de passe. Un second facteur d'authentification (2FA) est une fonctionnalité progressivement en cours de déploiement sur nos différentes applications.

Les applications développées par Gammadia permettent de définir précisément les données accessibles ou non pour chaque utilisateur. Il est de la responsabilité du client de définir sa politique de gestion des mots de passe, de sa bonne application ainsi que de la configuration adéquate des autorisations de ses propres utilisateurs.

En ce qui concerne les accès des collaborateurs aux différents systèmes de Gammadia, ils sont systématiquement protégés par une identification à double facteur. Les principes de privilège minimum sont également appliqués afin de limiter les accès.

7. Sauvegardes

Afin de pallier tout risque de perte de données, les bases de données de nos applications sont intégralement sauvegardées chaque heure et la procédure de restauration est régulièrement testée.

Les sauvegardes sont entreposées sur des sites distincts et sont conservées conformément à notre politique de rétention.

8. Mise à jour des systèmes

Nos systèmes sont mis à jour en permanence. De manière générale, la redondance de nos systèmes ainsi que nos procédures permettent d'effectuer les opérations de maintenance sans interruption de service. Des notifications préalables sont adressées par email à nos clients pour les cas où un arrêt des systèmes ne peut être évité.

9. Organisation interne

Gammadia a défini ses politiques et procédures de sécurité, lesquelles sont communiquées à l'ensemble du personnel. Les collaborateurs reçoivent une formation en matière de cybersécurité à leur engagement et sont régulièrement sensibilisés aux bonnes pratiques à observer en la matière.

La fonction de Responsable de la sécurité informatique est directement rattachée à la Direction. Un conseiller à la protection des données est également nommé.

10. Responsabilités

Conformément aux exigences légales en matière de protection des données, Gammadia maintient un registre de ses activités de traitement ainsi qu'un registre des incidents de sécurité.

Les principes de la **protection des données dès la conception et par défaut** sont appliqués pour tous les nouveaux développements. Des analyses d'impact sur la vie privée sont également menées lorsque la situation l'exige.

Unsere Sicherheitsverfahren

Wir legen grössten Wert darauf, ein vertrauenswürdiger Partner für unsere Kunden zu sein. Sicherheit ist daher ein grundlegendes Thema für gammadia AG.

Sämtliche Software von gammadia wird als Software-as-a-Service (SaaS) angeboten. Das heisst, wir übernehmen die Verantwortung für alle mit der Nutzung der Applikationen verbundenen Aspekte der Datensicherheit und Verfügbarkeit.

1. Gesetzeskonformität

Als Anbieter von Applikationen für seine Kundschaft übernimmt gammadia die Rolle eines Auftragsbearbeiters im Sinne des Bundesgesetzes über den Datenschutz (DSG). gammadia verpflichtet sich, die nach diesem Gesetz zu erfüllenden Anforderungen einzuhalten, und erklärt hier im Sinne der Transparenz die getroffenen organisatorischen und technischen Sicherheitsmassnahmen. In der «Vereinbarung über die Bearbeitung von Personendaten», die auf seiner Website verfügbar ist, wird genau beschrieben, wie gammadia in seiner Eigenschaft als Auftragsbearbeiter mit Personendaten umgeht.

2. Entwicklung und Hosting in der Schweiz

Die Applikationen von gammadia werden von den eigenen Entwicklern des Unternehmens in der Schweiz entwickelt. Die Lösungen und die darin enthaltenen Personendaten werden in Rechenzentren von ISO 27001-zertifizierten Dienstleistern in der Schweiz oder in Europa gehostet.

3. Datensicherheit

Die Daten werden während der Übertragung mithilfe des TLS-Protokolls verschlüsselt. Statische Daten, Benutzerkennungen und Back-ups werden ebenfalls mittels geeigneter Technologien verschlüsselt, die stets auf dem neuesten Stand gehalten werden.

4. Vertraulichkeit

Die Daten werden streng voneinander getrennt, um zu gewährleisten, dass die Informationen jeder Kundin und jedes Kunden vertraulich behandelt werden. Die Architektur unserer Applikationen garantiert, dass die Daten mittels spezieller Datenbanken und spezifisch abgegrenzter Bereiche geschützt werden. Ohne ausdrückliche Zustimmung unserer Kundinnen und Kunden werden keine Informationen an Dritte übertragen oder weitergegeben.

Unsere Mitarbeitenden sind vertraglich zur Wahrung des Berufsgeheimnisses verpflichtet.

5. Verfügbarkeit

Alle Bestandteile unserer Infrastruktur sind aufgrund der Redundanz unserer Systeme ausfallsicher. Unsere Dienste werden an 365 Tagen im Jahr rund um die Uhr von unserem Supportteam überwacht. Warnmeldungen werden Tag und Nacht umgehend bearbeitet. Unsere Systemwiederherstellungsverfahren versetzen uns in die Lage, unsere Dienste nach einem grösseren Vorfall rasch wiederherzustellen.

6. Zugriffskontrolle

Der Zugriff unserer Kundinnen und Kunden auf die Applikationen ist durch eine Kombination aus Benutzername und Passwort geschützt. Darüber hinaus führen wir in unseren verschiedenen Applikationen nach und nach die 2-Faktor-Authentifizierung (2FA) ein.

Mit den von gammadia entwickelten Applikationen kann genau festgelegt werden, auf welche Daten jede Benutzerin und jeder Benutzer zugreifen kann. Es liegt in der Verantwortung unserer Kundinnen und Kunden, Richtlinien für die Verwaltung von Passwörtern zu formulieren sowie deren ordnungsgemässe Anwendung und die angemessene Konfiguration der Benutzerberechtigungen sicherzustellen.

Der Zugriff der Mitarbeitenden auf die verschiedenen Systeme von gammadia wird systematisch durch 2-Faktor-Authentifizierung geschützt. Ausserdem wird der Zugriff durch Anwendung des Least-Privilege-Prinzips – d. h. Mitarbeitende erhalten nur die Berechtigungen, die sie wirklich benötigen – beschränkt.

7. Back-ups

Um das Risiko eines Datenverlusts weitestgehend zu mindern, wird stündlich ein Back-up der Datenbanken unserer Applikationen durchgeführt und die Wiederherstellung wird regelmässig getestet.

Die Back-ups werden an verschiedenen Standorten gespeichert und gemäss unserer Richtlinie zur Datenspeicherung aufbewahrt.

8. Systemupdates

Unsere Systeme werden durch Updates laufend aktualisiert. Dank der Redundanz unserer Systeme sowie unserer Verfahren können Wartungsarbeiten im Allgemeinen ohne Betriebsunterbruch durchgeführt werden. Ist eine Abschaltung unserer Systeme unvermeidbar, werden unsere Kundinnen und Kunden vorab per E-Mail benachrichtigt.

9. Interne Organisation

gammadia hat Sicherheitsrichtlinien und -verfahren festgelegt, mit denen sich alle Mitarbeitenden vertraut machen müssen. Neu eingestellte Mitarbeitende müssen eine Schulung zum Thema Cybersicherheit absolvieren. Zudem werden alle Mitarbeitenden regelmässig über bewährte Vorgehensweisen auf diesem Gebiet aufgeklärt.

Der Beauftragte für IT-Sicherheit ist unmittelbar der Geschäftsleitung unterstellt. Ausserdem wurde ein Datenschutzbeauftragter ernannt.

10. Pflichten von gammadia

Gemäss den gesetzlichen Datenschutzanforderungen führt gammadia ein Verzeichnis seiner Bearbeitungstätigkeiten sowie ein Verzeichnis von Sicherheitsvorfällen.

Die Grundsätze des **Datenschutzes durch Technik und datenschutzfreundliche Voreinstellungen** werden auf sämtliche neu entwickelte Software angewendet. Falls erforderlich, werden auch Datenschutz-Folgenabschätzungen durchgeführt.

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.