

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 chiffons 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.