Retour au Dossier Organisationnel	
Sujets connexes	Cartographie fonctionnelle de LoGeAs Proc#15 - Exercice des droits des personnes (RGPD) Proc#130 - Sauvegardes : plan, suivi et restauration Proc#134 - Charte d'utilisation des ressources informatiques CNIL : notifier une violation de données personnelles

Proc#181 - Faille de sécurité et violation de données : information des clients

Informations qualité

Suivi des modifications majeures		
Date	**Auteur**	**Modifications**
2026-10-02	Nicolas MARCHAND	Création, suite au point de vigilance n°12 de l'audit NF 552 de novembre 2025
Suivi des approbations	Cartographie fonctionnelle – fiche de la procédure	
Objet	Définir comment Logeas Informatique traite une faille de sécurité du logiciel LoGeAs ou de son infrastructure, et comment il en informe ses clients, afin qu'ils puissent remplir leurs propres obligations de notification à la CNIL et aux personnes concernées.	
Destinataires	**- Validation des modifications :** Gérant **- Approbation du document :** Gérance	

Champ d'application

Cette procédure s'applique à tout événement de sécurité touchant LoGeAs, ses serveurs ou les données qu'ils hébergent :

- une **faille de sécurité** : vulnérabilité découverte dans le logiciel ou l'infrastructure (signalée par un client, un partenaire comme Stoïk, un éditeur de composant ou détectée en interne), qu'elle ait été exploitée ou non ;
- une **violation de données personnelles** : destruction, perte, altération, divulgation ou accès non autorisé à des données personnelles, qu'elle soit accidentelle ou malveillante (article 4.12 du RGPD).

Pour les données contenues dans la base LoGeAs d'un client (ses membres, donateurs, contacts), Logeas Informatique est **sous-traitant** : c'est le client, responsable du traitement, qui notifie la CNIL et, le cas échéant, les personnes concernées. Logeas Informatique doit l'en informer **dans les meilleurs délais** (article 33.2 du RGPD).
Pour les données que Logeas Informatique traite pour son propre compte (comptes utilisateurs, échanges d'assistance, dossiers des salariés), il est **responsable du traitement** et notifie lui-même la CNIL.

Règles

- **Délai d'information des clients :** au plus tard **48 heures** après la prise de connaissance d'une violation de données touchant leurs bases, pour leur laisser le temps de notifier la CNIL dans les 72 heures que leur impose le RGPD (article 33.1). L'information peut être donnée en plusieurs fois si tous les éléments ne sont pas encore connus.
- **Faille non exploitée :** une faille corrigée sans indice d'exploitation n'est pas une violation de données. Les clients concernés sont informés si la faille les expose à un risque ou leur demande une action (mise à jour, changement de mot de passe).
- **Responsabilité :** le correspondant RGPD pilote la procédure, avec le correspondant infogérance pour l'analyse technique. La gérance décide de l'information des clients.
- **Traçabilité :** chaque événement est inscrit au **registre des violations**, tenu hors du wiki, y compris ceux qui n'ont pas donné lieu à notification (article 33.5 du RGPD).
- **Discrétion :** tant que la faille n'est pas corrigée, ses détails techniques ne sont communiqués qu'aux personnes qui en ont besoin.

Déroulé

Étape	Qui	Quoi
1. Signalement	Toute personne de l'équipe	Signaler immédiatement l'événement au correspondant RGPD et au correspondant infogérance, quelle que soit sa source (Proc#134). Ne pas chercher à le traiter seul.
2. Confinement	Correspondant infogérance	Limiter l'impact : isoler le serveur ou le compte concerné, couper l'accès, changer les secrets exposés. Conserver les traces (journaux, piste d'audit) avant toute remise en état.
3. Qualification	Correspondant RGPD, correspondant infogérance	Déterminer : la nature de l'événement (faille ou violation), les systèmes et les bases touchés, les catégories et le nombre approximatif de personnes et d'enregistrements concernés, les conséquences probables. Noter la date et l'heure de prise de connaissance, point de départ des délais.
4. Décision	Gérance	Décider de l'information des clients et, si Logeas Informatique est responsable du traitement, de la notification à la CNIL.
5. Information des clients	Correspondant RGPD	Informer chaque client concerné par courriel à son administrateur, depuis une boîte partagée (Proc#10), dans le délai fixé ci-dessus. Le message comprend les éléments listés ci-dessous.
6. Notification CNIL (cas responsable du traitement)	Correspondant RGPD	Notifier la CNIL dans les 72 heures sur son téléservice, et informer les personnes concernées si la violation présente un risque élevé pour elles (article 34 du RGPD).
7. Correction	Développement, correspondant infogérance	Corriger la faille ; si la correction passe par une nouvelle version, suivre Proc#168. Si des données doivent être restaurées, suivre Proc#130.
8. Clôture	Correspondant RGPD	Compléter le registre, informer les clients de la correction, et tirer les enseignements de l'événement (action corrective, mise à jour d'une procédure).

Contenu de l'information au client

Conformément à l'article 33.3 du RGPD, le message au client indique, autant que possible :

- la nature de l'événement, la date de sa survenue et celle de sa découverte ;
- les catégories et le nombre approximatif de personnes et d'enregistrements concernés dans sa base ;
- les conséquences probables ;
- les mesures prises ou envisagées pour y remédier et en limiter les effets ;
- les actions recommandées au client (par exemple changer les mots de passe) ;
- le nom et les coordonnées du correspondant RGPD de Logeas Informatique.

Le client doit pouvoir s'appuyer sur ce message pour sa propre notification à la CNIL.

Registre des violations

Le registre est un enregistrement tenu dans le cloud de l'entreprise, hors du wiki. Pour chaque événement, il indique : la date de prise de connaissance, la description, les bases et clients concernés, la qualification (faille ou violation), les décisions prises et leurs motifs, les dates d'information des clients et, le cas échéant, de notification à la CNIL, les mesures correctives.

From:
https://wiki-logeas.fr/certif/ - **dokuwiki-certif**

Permanent link:
https://wiki-logeas.fr/certif/doku.php?id=certif:procedure:violationdonnees

Last update: **2026/10/02 15:08**