RGPD et protection des données - AccessManager

Référence	AM-DOC-GU-001
Révision	1.1
Date	2026-08-27
Projet	AccessManager
Statut de maturité	Validé
Nombre de pages (annexes incluses)	4

Table des matières

1. Responsable du traitement

Le responsable du traitement des données personnelles est l'organisation utilisant AccessManager.

2. Données collectées

Dans le cadre de la gestion des accès, les données suivantes sont collectées :

- **Utilisateurs de l'application** : nom, prénom, email, identifiant, rôles
- **Demandes d'accès** : nom, prénom, email, téléphone, date de naissance, lieu de naissance, entreprise, photo, carte d'identité (conservation réduite, voir ci-dessous)
- **Données techniques** : logs de connexion, historique des actions

3. Finalité du traitement

Les données sont collectées pour les finalités suivantes :

- Gestion et contrôle des accès aux installations
- Vérification d'identité et sécurité
- Traçabilité des entrées et sorties
- Communication avec les demandeurs d'accès

4. Base légale

Le traitement est fondé sur :

- L'intérêt légitime de l'organisation (sécurité des installations)
- Le consentement de la personne concernée
- L'obligation légale (traçabilité des accès)

5. Durée de conservation

Les données sont conservées pendant la durée nécessaire aux finalités pour lesquelles elles sont collectées :

- **Demandes d'accès** : durée de validité de l'accès + archive selon réglementation
- **Carte d'identité** : supprimée dès le contrôle de saisie ; au plus tard 15 jours après la date de départ prévue si la demande n'est jamais vérifiée (voir ci-dessous)
- **Données utilisateurs** : durée d'utilisation du compte + obligations légales
- **Logs** : 12 mois maximum

5.1. Suppression anticipée de la carte d'identité

La copie de la pièce d'identité est la donnée la plus sensible du dossier. Elle n'a qu'une finalité : permettre au secrétariat de **vérifier que le visiteur a saisi correctement** son identité. Le criblage, lui, porte sur l'identité déclarée et non sur le document.

En application du principe de minimisation, elle est donc **supprimée automatiquement dès que le contrôle de saisie est effectué**, sans attendre la fin de validité de l'accès.

5.1.1. Délais de conservation

La durée de conservation n'est pas fixée par un délai calendaire mais par un **événement** : la vérification de la saisie par le secrétariat.

- **Délai minimal : aucun.** La suppression intervient dès la vérification, qui peut suivre la saisie de quelques minutes. Aucune durée plancher n'est appliquée : la donnée n'est pas conservée « au moins » un certain temps.
- **Cas courant :** de quelques heures à quelques jours, le temps que le secrétariat contrôle le dossier.
- **Délai maximal : 15 jours après la date de départ prévue.** Si une demande n'est jamais vérifiée, elle est supprimée en totalité — pièce d'identité comprise — par la purge automatique des accès expirés. Ce seuil de 15 jours est la valeur par défaut de la purge et peut être réduit par l'exploitant.

La suppression est définitive : elle porte sur la donnée chiffrée en base, qu'aucune sauvegarde applicative ne conserve par ailleurs. Si une demande déjà vérifiée devait être renvoyée en saisie, le visiteur serait invité à fournir à nouveau sa pièce d'identité.

La **photo** d'identité, elle, est conservée pendant la validité de l'accès : elle figure sur le badge présenté à l'entrée.

6. Droits des personnes

Conformément au RGPD, vous disposez des droits suivants :

- **Droit d'accès** : obtenir une copie de vos données
- **Droit de rectification** : corriger vos données inexactes
- **Droit à l'effacement** : demander la suppression de vos données
- **Droit à la limitation** : limiter le traitement de vos données
- **Droit d'opposition** : vous opposer au traitement de vos données
- **Droit à la portabilité** : récupérer vos données dans un format structuré

Pour exercer ces droits, contactez le responsable du traitement de votre organisation.

7. Sécurité des données

Des mesures techniques et organisationnelles sont mises en œuvre :

- Chiffrement des mots de passe (hashage sécurisé)
- Protection CSRF contre les attaques
- Limitation des tentatives de connexion
- Gestion des rôles et droits d'accès
- Stockage sécurisé des données sensibles
- Sauvegarde régulière des données

8. Cookies utilisés

L'application utilise uniquement des cookies techniques nécessaires :

- Cookie de session PHP (PHPSESSID) : authentification et navigation
- Cookie CSRF : protection contre les attaques CSRF

Aucun cookie de traçage, analytique ou publicitaire n'est utilisé.

9. Transfert de données

Les données ne sont pas transférées hors de l'organisation.

10. Réclamation

Vous pouvez introduire une réclamation auprès de la CNIL (`https://www.cnil.fr`) si vous estimez que le traitement de vos données n'est pas conforme au RGPD.