



EventsManager

RGPD et protection des données

Réf. EVM-DOC-RGPD-001 • Version 1.4 • 16/09/2026



REY CONSEILS



**Contrôle d'accès
sécurisé**



**Accès rapide
et fluide**



**Gestion simplifiée
des utilisateurs**



**Solution Web
accessible partout**

Table des matières

1	Objet	2
2	Responsable du traitement	2
3	Données collectées	2
3.1	Invités et accompagnants	2
3.2	Utilisateurs de l'application	2
3.3	Données techniques	2
3.4	Interdictions d'accès	3
4	Finalité du traitement	3
5	Base légale	3
6	Destinataires	3
7	Durée de conservation	4
8	Archive des visites d'un site sensible	4
8.1	Contenu	4
8.2	Constitution et accès	4
8.3	Protection et conservation	4
8.4	Exercice des droits	5
9	Interdictions d'accès	5
9.1	Aucune identité conservée	5
9.2	Qualification du traitement	5
9.3	Absence de décision entièrement automatisée	5
9.4	Exercice des droits	5
10	Droits des personnes	6
11	Sécurité des données	6
12	Cookies utilisés	6
13	Transfert de données	7
14	Réclamation	7

1. Objet

EventsManager est une application de gestion d'événements et d'invitations. Elle traite des données à caractère personnel concernant les invités, leurs accompagnants et les utilisateurs de l'application. Le présent document décrit ces traitements et les droits des personnes concernées.

2. Responsable du traitement

Le responsable du traitement est l'organisation qui utilise EventsManager pour organiser ses événements. L'application est multi-organisations : chaque organisation est responsable des seules données de ses propres événements, et n'a accès à aucune donnée d'une autre organisation.

3. Données collectées

3.1. Invités et accompagnants

- **Identité** : civilité, nom, prénom ;
- **Coordonnées** : adresse de courriel, téléphone ;
- **Éléments d'identification** : date et lieu de naissance, fonction, entreprise (facultative, déclarée par le référent) ;
- **Service invitant** : service de l'organisation qui invite la personne, renseigné par l'import de la liste ;
- **Participation** : réponse à l'invitation, réponses au questionnaire, date et heure d'arrivée (check-in) ;
- **Contrôle d'accès** : statut du criblage, date du contrôle, appartenance au personnel du ministère des Armées le cas échéant ;
- **Accessibilité** : indication « personne à mobilité réduite », déclarée par l'intéressé ou saisie par le gestionnaire. Elle sert le seul accueil sur place — stationnement, cheminement — et n'est transmise ni au criblage, ni au service de sécurité ;
- **Rattachement** : référent ayant invité la personne, le cas échéant ;
- **Traçabilité de la demande d'accès** : nom et prénom de l'utilisateur à l'origine de la demande (gestionnaire qui a créé, importé ou accepté l'invité) et de l'agent qui a validé le criblage.

3.2. Utilisateurs de l'application

Identifiant, civilité, nom, prénom, adresse de courriel, rôles, organisation de rattachement, état du compte. Les mots de passe ne sont pas conservés en clair : seule une empreinte est stockée.

Le nom et le prénom du gestionnaire à l'origine d'une demande d'accès et de l'agent qui l'a validée sont en outre enregistrés sur l'invité concerné. Ils y demeurent si le compte est supprimé, et figurent dans l'archive des visites (section 8).

3.3. Données techniques

Journal des courriels émis (destinataire, sujet, corps, statut, éventuel motif d'échec, pièces jointes), nécessaire au suivi des envois et au réémission en cas d'échec.

Historique des événements : date, auteur, organisation, nature de l'événement, objet visé et **adresse IP** d'origine, pour les connexions et échecs de connexion, les verrouillages de compte, les accès refusés, les actions d'administration sur les comptes et les organisations, et les exports de données. Il assure l'imputabilité des accès et des actions d'administration.

Aucun mot de passe n'y figure, sous aucune forme : celui qui est saisi lors d'une tentative de connexion n'est jamais conservé, même en cas d'échec. En revanche, l'**identifiant saisi** l'est — y compris lorsqu'il ne correspond à aucun compte, cas qui signale une tentative de deviner des identifiants.

3.4. Interdictions d'accès

Aucune identité : une **empreinte pseudonymisée** de l'état civil et une date d'échéance. Voir la section consacrée à ce registre.

4. Finalité du traitement

- Constitution et gestion des listes d'invités d'un événement ;
- Envoi des invitations, des informations et des billets d'accès (e-tickets) ;
- Recueil des réponses et des contraintes des participants (questionnaire) ;
- Délégation d'invitations à des référents ;
- Contrôle d'accès le jour de l'événement (lecture du QR code, enregistrement des arrivées) ;
- Lorsque l'événement se tient sur un site sensible, transmission au service de sécurité des éléments nécessaires à l'autorisation d'accès ;
- Sur un site sensible, **archivage des visites** à des fins de sécurité du site et de statistiques (section 8).

5. Base légale

- **Intérêt légitime** de l'organisation : organisation de l'événement et sécurité du site, y compris la conservation de l'archive des visites ;
- **Consentement** de la personne concernée : réponse à l'invitation et au questionnaire, communication de sa date et de son lieu de naissance en vue du criblage ;
- **Obligation légale** : contrôle et traçabilité des accès sur les sites soumis à une réglementation particulière.

6. Destinataires

- Les utilisateurs habilités de l'organisation, selon leur rôle (voir le guide utilisateur) ;
- Le **service de sécurité**, destinataire des seules données nécessaires à l'autorisation d'accès : nom, prénom, date de naissance et lieu de naissance des invités ayant confirmé leur participation et non dispensés de criblage ;
- Les **deux responsables de la sécurité du site**, seuls destinataires de l'archive des visites ;
- L'hébergeur, en qualité de sous-traitant technique.

7. Durée de conservation

- **Données des invités** : durée de l'événement, puis conservation limitée aux besoins de traçabilité des accès; la suppression d'un événement supprime les invités et leurs réponses ;
- **Réponses au questionnaire** : supprimées avec l'invité auquel elles se rattachent ;
- **Journal des courriels** : conservé le temps du suivi des envois, purgeable depuis l'application ;
- **Historique des événements** : **un an**, puis suppression automatique quotidienne. Il n'est effaçable depuis aucun écran : une trace que l'on pourrait retirer ne prouverait rien ;
- **Comptes utilisateurs** : durée d'utilisation du compte ;
- **Interdictions d'accès** : jusqu'au terme fixé par la décision, puis suppression automatique quotidienne ;
- **Archive des visites d'un site sensible** : **cinq ans** à compter de la date de la visite, dans un coffre chiffré hors de l'application, puis destruction. Cette durée est indépendante de celle des données de l'événement : la suppression d'un événement dans l'application n'efface pas l'archive déjà constituée.

8. Archive des visites d'un site sensible

Lorsque les événements se tiennent sur un site sensible ouvert au public, la liste des visiteurs est archivée pour permettre, a posteriori, de savoir qui a eu accès au site, à quelle date, à la demande de qui et sur l'avis de qui — et d'en établir des statistiques.

8.1. Contenu

Pour chaque visiteur dont l'accès était autorisé (criblage validé, ou dispense accordée au personnel du ministère des Armées) : **nom, prénom, date et lieu de naissance, date de la visite, auteur de la demande, agent qui l'a validée**. Aucune coordonnée, aucune réponse au questionnaire, aucune donnée de participation n'y figure.

8.2. Constitution et accès

- L'archive est constituée par un export périodique — en principe hebdomadaire — produit depuis l'application par un profil dédié, **responsable de la sécurité du site**, qui ne donne accès à aucune autre fonction ni à aucune autre donnée.
- Ce profil est attribué aux **deux seules personnes** responsables de la sécurité du site. Elles sont les seules à pouvoir produire l'export et à accéder au coffre.
- Chaque export est inscrit à l'historique de l'application (auteur, date, période, nombre de lignes).

8.3. Protection et conservation

- Dès son téléchargement, le fichier est **chiffré** et déposé dans un **coffre** dont l'accès est limité aux deux responsables, puis supprimé du poste de travail.
- L'application n'en conserve aucune copie.
- Chaque fichier est conservé **cinq ans** à compter de la date des visites qu'il recense, puis détruit.

8.4. Exercice des droits

Les droits d'accès, de rectification et de limitation s'exercent auprès du responsable du traitement, qui fait procéder à la recherche dans l'archive par les responsables de la sécurité du site. Le traitement reposant sur l'intérêt légitime, une demande d'opposition (article 21.1 du règlement) — et l'effacement qui en découlerait (article 17.1.c) — peut être écartée pendant la durée de conservation lorsque la sécurité du site constitue un motif légitime et impérieux ; la personne en est alors informée, avec le motif du refus.

9. Interdictions d'accès

Un avis défavorable du criblage peut être assorti d'une **interdiction d'accès** d'une durée déterminée : toute invitation ultérieure visant la même personne est alors arrêtée avant le criblage.

9.1. Aucune identité conservée

Le registre des interdictions ne contient **ni nom, ni prénom, ni date ou lieu de naissance**. La personne y est désignée par une **empreinte** calculée à partir de son état civil, qui présente trois propriétés :

- **Elle ne se lit pas à l'envers.** L'empreinte ne permet pas de retrouver l'identité — pas davantage pour un administrateur de l'application que pour quiconque accèderait à la base de données.
- **Elle est inutilisable hors de l'application.** Son calcul dépend d'une clé conservée sur les serveurs, jamais dans la base. Une copie de la base seule ne permet ni de lire les interdictions, ni de vérifier si une personne donnée y figure.
- **Elle ne renvoie à rien.** Aucun lien n'est enregistré entre une interdiction et l'invitation ou l'événement qui l'ont motivée.

9.2. Qualification du traitement

Ce mécanisme relève de la **pseudonymisation** au sens de l'article 4.5 du règlement, et non de l'anonymisation : une même identité produit toujours la même empreinte, ce qui est précisément ce qui permet de reconnaître une personne qui reviendrait. Les données du registre restent donc des données à caractère personnel, et le traitement figure au registre des activités.

La mesure technique retenue — condensat clavé — relève de l'état de l'art au sens de l'article 32.

9.3. Absence de décision entièrement automatisée

La décision d'interdire résulte d'un avis rendu par une autorité de criblage et saisi par un agent : l'application ne fait que l'exécuter. Le traitement n'entre donc pas dans le champ de l'article 22 du règlement.

9.4. Exercice des droits

L'identité n'étant pas conservée, l'exercice des droits sur ce registre suppose que la personne concernée fournisse son état civil : l'application recalcule alors l'empreinte et retrouve — ou non — l'interdiction la visant.

- **Droit d'accès** : la seule information communicable est l'existence d'une interdiction et sa date d'échéance.

- **Droit à l'effacement** : la levée supprime l'enregistrement, sans attendre le terme.
- **Limite** : deux personnes de mêmes nom, prénom, date et lieu de naissance produisent la même empreinte et sont traitées comme une seule. Le cas est rare mais doit être signalé au service de criblage.

10. 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 — un référent peut corriger directement les données de ses accompagnants depuis son espace ;
- **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 l'organisation qui vous a invité. L'organisateur dispose d'un export des données de l'événement permettant de répondre à une demande d'accès.

11. Sécurité des données

- **Chiffrement des données personnelles en base** : l'identité et les coordonnées des invités, l'auteur de leur demande d'accès et l'agent qui l'a validée, ainsi que les réponses au questionnaire, sont chiffrés. Le chiffrement est enveloppé : une clé propre à chaque organisation chiffre les données, et cette clé est elle-même protégée par une clé maître ;
- Les recherches sur les données chiffrées s'appuient sur des index aveugles, qui ne révèlent pas les valeurs ;
- **Cloisonnement** : une organisation n'accède jamais aux données d'une autre ;
- **Mots de passe** : stockés sous forme d'empreinte, jamais en clair ;
- **Contrôle d'accès** : rôles applicatifs et vérification systématique de l'appartenance des données à l'organisation de l'utilisateur ;
- Protection contre les attaques CSRF, limitation des tentatives de connexion, en-têtes de sécurité restrictifs (dont une politique de sécurité de contenu) ;
- Journalisation des accès, des refus d'accès et des actions d'administration, cloisonnée par organisation ;
- Communication chiffrée (HTTPS) ;
- Sauvegardes régulières.

12. Cookies utilisés

L'application n'utilise que des cookies techniques nécessaires à son fonctionnement :

- cookie de session (PHPSESSID) : authentification et navigation ;
- jeton CSRF : protection contre la falsification de requête.

Aucun cookie de traçage, de mesure d'audience ou de publicité n'est utilisé.

13. Transfert de données

Les données sont hébergées en France et ne font l'objet d'aucun transfert hors de l'Union européenne.

En dehors de l'organisation, la seule transmission est celle décrite à la section « Destinataires » : l'envoi au service de sécurité des éléments d'identité strictement nécessaires à l'autorisation d'accès, lorsque l'événement se tient sur un site sensible.

L'archive des visites sort de l'application mais ne quitte pas l'organisation : elle est conservée dans son coffre, sous la seule responsabilité des responsables de la sécurité du site.

14. 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.