

GUIDE PRATIQUE

Comment protéger les données des salariés collectées par le CSE ?

Article 67 - Protection des données (RGPD) pour le CSE

Finalité du guide	Donner aux élus une méthode opérationnelle pour collecter, utiliser, partager et supprimer les données des salariés avec un niveau de sécurité adapté aux risques.
Public cible	Élus CSE, secrétaire, trésorier, commissions, gestionnaires ASC, bénévoles et référent RGPD du CSE.
Usage recommandé	ASC, inscriptions, billetterie, voyages, aides sociales, enquêtes, réclamations, newsletters, événements et fichiers de contacts.
Résultat attendu	Moins de données inutiles, moins d'exports dispersés, des accès maîtrisés, des suppressions planifiées et une confiance renforcée des salariés.

Message central

Protéger les données ne consiste pas à tout conserver « au cas où ». Le bon réflexe est de limiter la collecte, sécuriser les accès, encadrer les outils, fixer une durée de conservation et supprimer ce qui n'est plus nécessaire.

- Traiter chaque fichier comme un actif à protéger : responsable, finalité, accès, durée, sécurité.
- Éviter les fichiers Excel diffusés par mail ou stockés sur des espaces personnels.
- Renforcer la protection dès qu'un fichier contient des informations de santé, des données sociales détaillées ou des informations concernant des enfants.
- Sensibiliser tous les élus et bénévoles : la sécurité dépend autant des pratiques que des outils.

CFE-CGC Mutualité | Protection des données, confiance et responsabilité

Sommaire

- 1. Identifier les données réellement nécessaires**
- 2. Classer les données selon leur niveau de risque**
- 3. Sécuriser les accès, comptes et appareils**
- 4. Maîtriser les fichiers, exports et partages**
- 5. Fixer des durées de conservation et supprimer**
- 6. Encadrer les prestataires et les incidents**
- 7. Installer une gouvernance simple de sécurité**
- 8. Checklists, modèles et plan d'action 30 jours**

Principe directeur

L'article 32 du RGPD impose des mesures techniques et organisationnelles adaptées au risque. Il n'existe donc pas une mesure unique : le CSE doit proportionner la sécurité à la nature des données, au nombre de personnes concernées et aux conséquences possibles d'une fuite ou d'un accès non autorisé.

1. Identifier les données réellement nécessaires

La première mesure de sécurité est de ne pas collecter inutilement

Avant chaque formulaire, fichier ou nouvelle prestation, le CSE doit distinguer les informations indispensables de celles simplement « pratiques ». Moins une donnée est collectée et conservée, moins elle peut être exposée.

Usage	Données souvent utiles	À éviter ou à limiter
Billetterie / ASC	Identité, ouvrant droit, élément nécessaire au calcul du droit	Copies intégrales de justificatifs conservées sans nécessité
Voyage / événement	Coordonnées, contraintes logistiques utiles	Informations privées sans lien avec l'organisation
Aide sociale	Éléments strictement nécessaires à l'instruction	Diffusion du dossier à un grand nombre d'élus
Enquête	Réponses nécessaires à l'objectif	Questions identifiantes si une donnée agrégée suffit
Newsletter	Coordonnée de contact adaptée	Fichiers de diffusion dupliqués sur plusieurs postes

Trois questions avant toute collecte

- Cette donnée est-elle indispensable à la finalité annoncée ?
- Puis-je vérifier l'information sans conserver le justificatif ?
- Puis-je agréger ou anonymiser l'information plus tôt dans le processus ?

Point de vigilance

La situation familiale n'est pas, en elle-même, une « catégorie particulière » de données au sens de l'article 9 du RGPD. Elle reste néanmoins une information personnelle à protéger. Les données de santé, l'appartenance syndicale, les opinions politiques, la religion ou l'orientation sexuelle bénéficient d'une protection renforcée.

2. Classer les données selon leur niveau de risque

Adapter les protections au contenu et à l'usage

Niveau	Exemples	Mesures attendues
Courant	Nom, prénom, email professionnel, inscription simple	Accès nominatif, mot de passe robuste, durée définie
Renforcé	Revenus, quotient, situation familiale détaillée, coordonnées personnelles	Accès restreint, stockage centralisé, exports limités
Élevé	Santé, handicap, données syndicales, dossiers sociaux sensibles	Besoin strict, chiffrement/outil sécurisé, accès au minimum, traçabilité
Vulnérabilité accrue	Données concernant des enfants ou personnes fragiles	Minimisation maximale, prudence sur partage et conservation

Matrice de risque rapide

Question	Faible	Élevé
Combien de personnes sont concernées ?	Petit volume	Fichier massif
Que se passe-t-il en cas de fuite ?	Gêne limitée	Atteinte financière, sociale ou à la réputation
Les données sont-elles sensibles ?	Non	Oui ou informations très intimes
Les données sont-elles largement accessibles ?	2-3 personnes habilitées	Nombreux élus, bénévoles ou prestataires

Réflexe élu

Plus le risque est élevé, plus il faut réduire la donnée, réduire les accès, renforcer l'authentification, protéger le stockage et raccourcir la conservation.

3. Sécuriser les accès, comptes et appareils

La majorité des incidents vient de pratiques ordinaires

Risque courant	Mesure de base	Quick win
Mot de passe partagé	Un compte nominatif par utilisateur	Activer l'authentification multifacteur (MFA)
Départ d'un élu	Retrait immédiat des droits	Checklist de sortie le jour du changement
PC personnel non maîtrisé	Privilégier un équipement ou espace sécurisé	Verrouillage automatique + chiffrement
Lien de partage public	Accès nominatif et limité dans le temps	Revue trimestrielle des partages
Boîte mail commune	Droits individualisés	MFA + procédure de délégation
Support papier	Armoire fermée / accès limité	Destruction sécurisée en fin de conservation

Règles simples à formaliser

- Aucun mot de passe transmis par mail ou messagerie instantanée.
- Pas de téléchargement local si l'usage peut rester dans l'outil sécurisé.
- Verrouillage systématique des sessions et interdiction des comptes génériques non tracés.
- Revue des habilitations au moins chaque trimestre et après tout changement de mandat.
- Sauvegarde des données critiques et test périodique de restauration.

Objectif sécurité

Savoir répondre à deux questions à tout moment : « qui peut voir cette donnée ? » et « pourquoi cette personne en a-t-elle besoin ? »

4. Maîtriser les fichiers, exports et partages

L'export Excel est utile mais devient vite un angle mort

Pratique à risque	Alternative recommandée
Envoyer une liste complète en pièce jointe	Lien sécurisé avec accès nominatif et expiration
Copier un fichier sur plusieurs postes	Référentiel unique dans l'espace sécurisé
Télécharger « pour travailler plus vite »	Travailler dans l'outil quand c'est possible
Conserver toutes les versions	Version active + archivage maîtrisé
Utiliser une clé USB non chiffrée	Éviter le support amovible ou utiliser un support chiffré
Partager une liste à un prestataire sans filtre	Transmettre uniquement les champs nécessaires

5. Fixer des durées de conservation et supprimer

Le RGPD interdit la conservation indéfinie par défaut. Le CSE doit prévoir pour chaque traitement une durée cohérente avec la finalité, les obligations légales éventuelles et les besoins de preuve.

Étape	Action
1. Définir	Fixer la durée dès la création du fichier.
2. Automatiser	Utiliser, si possible, des règles d'expiration ou d'archivage.
3. Revoir	Identifier chaque trimestre les dossiers clos et exports inutiles.
4. Supprimer	Détruire de manière sécurisée les fichiers et supports devenus inutiles.

Bon réflexe

Une donnée supprimée au bon moment ne peut plus être volée, diffusée par erreur ou consultée par une personne qui n'en a plus besoin.

6. Encadrer les prestataires et les incidents

Le CSE reste responsable de ses choix de prestataires

Avant de confier des données	À vérifier
Contrat	Clauses de sous-traitance conformes à l'article 28 du RGPD
Sécurité	MFA, chiffrement, sauvegardes, journalisation, gestion des vulnérabilités
Sous-traitants ultérieurs	Information et encadrement
Localisation	Hébergement et transferts éventuels hors EEE
Fin de contrat	Restitution et suppression des données
Incident	Délai d'alerte du CSE et assistance à l'analyse

En cas de perte, erreur d'envoi ou accès indu

- 1 Stopper ou limiter l'exposition : retrait du lien, changement de mot de passe, blocage du compte.
- 2 Documenter : données concernées, volume, personnes, durée d'exposition, cause.
- 3 Évaluer le risque pour les droits et libertés des personnes.
- 4 Décider de la notification à la CNIL dans les 72 heures lorsque le RGPD l'exige et, si le risque est élevé, de l'information des personnes concernées.
- 5 Corriger la cause et conserver le retour d'expérience.

Ne pas improviser

Préparer avant l'incident une fiche réflexe avec les coordonnées du référent, du secrétaire, du prestataire concerné et du conseil juridique ou RGPD mobilisable.

7. Gouvernance, checklist et plan d'action

Checklist avant ouverture d'un fichier ou d'un outil

Question	Oui / Non	Action si non
La finalité et les données nécessaires sont-elles définies ?		Réduire le périmètre.
Le niveau de risque est-il qualifié ?		Classer le traitement.
Les accès sont-ils nominatifs et limités ?		Revoir les habilitations.
La MFA est-elle activée lorsque disponible ?		L'activer.
Les exports sont-ils évités ou maîtrisés ?		Centraliser les données.
La durée de conservation est-elle fixée ?		Définir suppression/archivage.
Le prestataire est-il encadré ?		Vérifier contrat et sécurité.
La procédure incident est-elle connue ?		Formaliser le circuit d'alerte.

Plan d'action 30 jours

Jalon	Action	Livrable
J+7	Recenser fichiers, exports, outils et accès	Cartographie des données
J+15	Identifier les traitements à risque élevé	Top 5 risques sécurité
J+21	Activer MFA, réduire les droits, nettoyer les exports	Plan correctif rapide
J+30	Valider charte interne, durées et rituel de revue	Dispositif de protection CSE

KPI simples

- % des comptes sensibles protégés par MFA.
- % des accès revus au cours des 3 derniers mois.
- Nombre d'exports Excel actifs hors espace sécurisé.
- % des traitements avec durée de conservation définie.
- Nombre d'incidents et délai moyen de traitement.

À retenir

La protection des données est un acte de responsabilité du CSE. Le meilleur dispositif combine minimisation, accès maîtrisés, outils sécurisés, suppression régulière et culture commune de confidentialité.

Références de travail

- Règlement (UE) 2016/679 : art. 5 (principes), art. 9 (catégories particulières), art. 25 (protection dès la conception), art. 28 (sous-traitants), art. 32 (sécurité), art. 33-34 (violations de données).
- CNIL : Guide de la sécurité des données personnelles ; mots de passe et authentification multifacteur ; registre des traitements ; violations de données.

CFE-CGC Mutualité | Réflexe élu : minimiser - sécuriser - limiter - supprimer