

GUIDE PRATIQUE

Le CSE et le RGPD

Quelles obligations légales pour les élus ?

Finalité du guide	Donner aux élus du CSE une méthode simple pour sécuriser leurs traitements de données personnelles et intégrer le RGPD dans le fonctionnement quotidien de l'instance.
Public cible	Élus titulaires et suppléants, secrétaire, trésorier, commissions, gestionnaires des ASC, référent RGPD du CSE et prestataires.
Usage recommandé	Gestion des ASC, listes de bénéficiaires, enquêtes, réclamations individuelles, événements, élections, newsletters, fichiers de contacts et plateformes en ligne.
Résultat attendu	Des traitements utiles, proportionnés, documentés et sécurisés ; des responsabilités claires ; une confiance renforcée des salariés.

Message central

Dès qu'il décide pourquoi et comment un fichier de données personnelles est utilisé, le CSE doit raisonner comme un responsable de traitement : finalité, base légale, minimisation, information, durée de conservation, sécurité et droits des personnes.

- Ne collecter que les données réellement nécessaires à la mission ou au service rendu.
- Séparer les fichiers de gestion du CSE des fichiers syndicaux : finalités, responsables et accès ne sont pas les mêmes.
- Encadrer les prestataires : billetterie, chèques-cadeaux, voyages, sondages, hébergement ou mailing.
- Documenter les choix et pouvoir démontrer la conformité en cas de contrôle ou de demande d'un salarié.

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

Sommaire

- 1. Qualifier le rôle du CSE au regard du RGPD**
- 2. Cartographier les traitements et choisir une base légale**
- 3. Informer les salariés et respecter leurs droits**
- 4. Sécuriser les données et maîtriser les accès**
- 5. Encadrer les prestataires et outils numériques**
- 6. Gérer les données sensibles et les incidents**
- 7. Piloter la conformité avec un dispositif simple**
- 8. Modèles, checklists et plan d'action 30 jours**

Principe directeur

Le RGPD ne vise pas à empêcher le CSE d'agir. Il impose de pouvoir expliquer pour chaque fichier : pourquoi il existe, quelles données sont nécessaires, qui y accède, combien de temps elles sont conservées et comment les personnes exercent leurs droits.

1. Qualifier le rôle du CSE au regard du RGPD

Le CSE peut être responsable de traitement pour ses propres activités

Le responsable de traitement est l'organisme qui détermine les finalités et les moyens essentiels d'un traitement. Lorsqu'il organise ses ASC, gère une newsletter, tient un fichier de bénéficiaires ou mène une enquête, le CSE doit donc qualifier son rôle au cas par cas.

Situation	Qualification à vérifier	Réflexe élu
Gestion des ASC par le CSE	CSE généralement responsable du traitement	Définir finalité, données, accès, conservation et information.
Prestataire de billetterie agissant sur instruction	Sous-traitant du CSE	Contrat RGPD, garanties de sécurité et sous-traitants ultérieurs.
Enquête menée conjointement avec un autre acteur	Responsabilité conjointe possible	Formaliser qui informe, répond aux droits et gère les incidents.
Fichier d'adhérents d'une section syndicale	Traitement syndical distinct du CSE	Ne pas mélanger les bases ni les accès.

Les 7 questions à poser avant de créer un fichier

- Quelle finalité précise ?
- Quelle base légale ?
- Quelles données strictement nécessaires ?
- Qui doit réellement y accéder ?
- Quelle durée de conservation ?
- Quelle information remettre aux salariés ?
- Quel niveau de sécurité et quelle procédure en cas d'incident ?

Point de vigilance

La désignation d'un « référent RGPD » au sein du CSE est une bonne pratique d'organisation, mais elle ne doit pas être confondue avec la désignation d'un DPO, qui n'est pas automatiquement obligatoire pour tout CSE.

2. Cartographier les traitements et choisir une base légale

Le registre transforme le RGPD en outil de pilotage

Le registre des traitements permet de centraliser les décisions et d'éviter les fichiers « historiques » dont plus personne ne connaît l'utilité. Il doit être tenu à jour dès lors que les obligations de l'article 30 du RGPD s'appliquent ; dans tous les cas, il constitue une pratique de référence pour documenter la conformité.

Traitement CSE	Finalité possible	Données à limiter	Base légale à documenter
ASC / billetterie	Attribuer un avantage et contrôler l'éligibilité	Identité, ouvrant droit, justificatifs nécessaires	Obligation/mission du CSE ou intérêt légitime selon le cas
Newsletter CSE	Informar les salariés	Nom, prénom, adresse professionnelle	Base à déterminer selon le canal et le contexte
Enquête QVCT	Mesurer une situation collective	Réponses minimisées, idéalement anonymes	Intérêt légitime ou mission selon le dispositif
Réclamations individuelles	Suivre une demande et défendre les intérêts	Faits et pièces strictement utiles	Mission du CSE ; attention aux données sensibles
Événements / voyages	Inscrire et gérer les participants	Coordonnées, besoins logistiques nécessaires	Contrat / gestion du service selon le cas

KPI de conformité utiles

- % de traitements recensés dans le registre.
- % de fichiers avec durée de conservation définie.
- Nombre de traitements contenant des données sensibles.
- Nombre d'accès ouverts à des élus ou prestataires non justifiés.
- Nombre de traitements supprimés ou simplifiés après revue annuelle.

Règle de minimisation

Un justificatif peut être nécessaire pour ouvrir un droit sans qu'il soit nécessaire d'en conserver une copie. Toujours distinguer « vérifier » une information de « stocker » durablement le document qui la prouve.

3. Informer les salariés et respecter leurs droits

Une information claire avant ou au moment de la collecte

Les personnes doivent comprendre qui utilise leurs données, pour quoi faire, pendant combien de temps, avec quels destinataires et comment exercer leurs droits. L'information doit être accessible, concise et adaptée au support utilisé.

Mention à prévoir	Question à laquelle répondre
Responsable du traitement	Qui porte le traitement au sein du CSE ?
Finalité et base légale	Pourquoi les données sont-elles utilisées et sur quel fondement ?
Données et destinataires	Quelles informations sont utilisées et par qui ?
Durée de conservation	Quand les données seront-elles supprimées ou archivées ?
Droits	Comment demander accès, rectification, effacement, limitation ou opposition lorsque applicable ?
Réclamation	Comment contacter la CNIL si nécessaire ?

Circuit recommandé pour une demande de droit

- 1 Réceptionner et dater la demande.
- 2 Vérifier l'identité de manière proportionnée.
- 3 Identifier les traitements concernés.
- 4 Répondre dans le délai RGPD applicable, en principe un mois.
- 5 Tracer la réponse et les éventuelles actions correctives.

Quick win

Créer une adresse fonctionnelle dédiée (ex. rgpd-cse@...) et une courte notice de confidentialité unique, réutilisable sur les formulaires ASC, enquêtes et inscriptions.

4. Sécuriser les données et maîtriser les accès

La sécurité doit être proportionnée à la sensibilité des informations

Risque	Mesure minimale	Mesure renforcée
Fichier partagé trop largement	Droits d'accès nominatifs	Revue trimestrielle des habilitations
Ordinateur ou compte partagé	Compte individuel + verrouillage	MFA et chiffrement du poste
Pièces justificatives sensibles	Stockage restreint	Suppression après contrôle si la copie n'est pas nécessaire
Envoi de listes par mail	Limiter les destinataires	Lien sécurisé plutôt que pièce jointe
Départ d'un élu	Retirer immédiatement les accès	Procédure de sortie documentée
Incident / fuite	Alerte interne immédiate	Analyse du risque et notification CNIL sous 72 h si requise

Données sensibles : vigilance maximale

Les données révélant notamment la santé, l'appartenance syndicale, les opinions politiques, la religion ou l'orientation sexuelle bénéficient d'une protection renforcée. Leur collecte doit être évitée lorsqu'elle n'est pas indispensable et juridiquement fondée.

Exemple ASC

Pour appliquer un quotient familial, privilégier le calcul ou la saisie de la tranche utile plutôt que la conservation indéfinie d'un avis d'imposition complet.

Réflexe incident

- Isoler le fichier ou le compte concerné.
- Documenter : données, personnes, durée, cause et destinataires.
- Évaluer le risque pour les personnes.
- Décider et tracer les notifications requises, avec l'appui du DPO de l'entreprise uniquement si le rôle de chacun le permet ou d'un conseil dédié au CSE.

5. Encadrer les prestataires et outils numériques

Le contrat doit traduire les obligations RGPD

Un prestataire qui traite des données pour le compte du CSE doit offrir des garanties suffisantes. Le contrat doit préciser l'objet, la durée, la nature du traitement, les catégories de données, la sécurité, l'assistance et le sort des données en fin de prestation.

À vérifier avant signature	Question pratique
Hébergement	Où sont stockées les données ? Y a-t-il des transferts hors EEE ?
Sous-traitants	Le prestataire en utilise-t-il et comment le CSE est-il informé ?
Sécurité	MFA, chiffrement, sauvegardes, journalisation, gestion des incidents ?
Droits des personnes	Le prestataire aide-t-il le CSE à répondre aux demandes ?
Fin de contrat	Suppression ou restitution documentée des données ?
Réversibilité	Peut-on récupérer les données dans un format exploitable ?

6. Gérer la conformité dans la durée

Le CSE peut piloter un dispositif léger mais robuste : un référent, un registre, une revue périodique et quelques indicateurs. L'objectif est d'éviter la conformité « papier » déconnectée des usages réels.

Rituel	Fréquence	Livrable
Revue des accès	Trimestrielle	Liste des habilitations à jour
Revue des traitements	Semestrielle	Registre mis à jour
Revue prestataires	Annuelle	Checklist sécurité / contrat
Sensibilisation des élus	À chaque renouvellement + rappel annuel	Support 30 minutes
Test incident	Annuel	REX et plan correctif

7. Modèles, checklist et plan d'action

Checklist CSE - avant de créer ou modifier un traitement

Question	Oui / Non	Action si non
La finalité est-elle formulée en une phrase ?		Clarifier l'usage attendu.
La base légale est-elle identifiée ?		Qualifier avec le référent / conseil.
Les données sont-elles toutes nécessaires ?		Supprimer les champs non utiles.
Les salariés sont-ils informés ?		Ajouter une notice de confidentialité.
La durée de conservation est-elle définie ?		Fixer suppression ou archivage.
Les accès sont-ils limités ?		Revoir les habilitations.
Le prestataire est-il encadré ?		Vérifier le contrat article 28.
La procédure incident est-elle connue ?		Nommer les contacts et le circuit d'alerte.

Plan d'action 30 jours

Jalon	Action	Livrable
J+7	Recenser les fichiers, outils et prestataires	Cartographie initiale
J+15	Prioriser les risques : données sensibles, volumes, accès	Top 5 risques RGPD
J+21	Mettre à jour information, accès et contrats prioritaires	Actions correctives
J+30	Valider gouvernance, rituels et KPI	Mini-plan de conformité CSE

À retenir

Le RGPD n'est pas un frein aux missions du CSE : c'est une méthode de maîtrise des données. Un CSE conforme collecte moins, explique mieux, sécurise davantage et sait démontrer ses choix.

Références de travail

- Règlement (UE) 2016/679 : principes, droits, responsabilité, registre, sécurité et sous-traitance.
- CNIL : registre des activités de traitement ; qualification responsable/sous-traitant ; sécurité et information des personnes.
- Code du travail : missions et moyens du CSE. Vérifier systématiquement les accords d'entreprise et règles internes applicables.

CFE-CGC Mutualité | Réflexe DS/élu : utile - proportionné - documenté - sécurisé