

GUIDE PRATIQUE

Exemple : un CSE ayant mis en place une politique RGPD efficace

Transformer la conformité en preuve de sérieux, de transparence et de confiance

Finalité du guide	Montrer, à travers un cas pédagogique, comment un CSE peut structurer une politique RGPD simple, progressive et durable sans transformer la conformité en projet administratif lourd.
Public cible	Élus du CSE, secrétaire, trésorier, commissions ASC, gestionnaires, référent RGPD, prestataires et personnes habilitées.
Usage recommandé	Lancement d'une démarche RGPD, renouvellement du CSE, audit interne, changement de logiciel ASC, revue des accès ou communication aux salariés.
Résultat attendu	Disposer d'une méthode reproductible : diagnostic, priorisation, sécurisation, formation, communication et pilotage par quelques indicateurs.

Important

Le cas présenté est un exemple pédagogique et anonymisé. Il illustre une démarche type à adapter à la taille du CSE, aux outils utilisés et aux données réellement traitées.

- Le point de départ : des fichiers dispersés, des accès trop larges et des règles de conservation peu formalisées.
- Le choix : traiter d'abord les risques concrets avant de produire des documents complexes.
- Le levier : un élu référent, des responsabilités claires et une revue trimestrielle courte.
- Le résultat : une meilleure maîtrise des données et une communication plus transparente auprès des salariés.

CFE-CGC Mutualité | RGPD, professionnalisation et confiance

Sommaire

- 1. Le point de départ : un CSE exposé sans le savoir**
- 2. Lancer un diagnostic simple et utile**
- 3. Prioriser les actions à fort impact**
- 4. Sécuriser les outils, accès et données ASC**
- 5. Former les élus et responsabiliser les usages**
- 6. Communiquer avec transparence aux salariés**
- 7. Mesurer les progrès et inscrire la démarche dans la durée**
- 8. Checklists, KPI et plan d'action reproductible**

Principe directeur

La conformité devient efficace lorsqu'elle est intégrée au fonctionnement courant du CSE : chaque nouveau fichier, nouvel outil, nouveau prestataire ou changement d' élu déclenche les mêmes réflexes de minimisation, sécurité et traçabilité.

1. Le point de départ

Un CSE actif, mais des pratiques devenues difficiles à maîtriser

Le CSE gère des prestations ASC, une newsletter, des inscriptions à des événements, des justificatifs de quotient familial et plusieurs prestataires. Avec le temps, les fichiers se sont multipliés et les règles sont devenues hétérogènes.

Constat initial	Risque associé	Décision prise
Plusieurs fichiers Excel locaux	Copies multiples, perte de maîtrise	Centraliser les données utiles
Comptes partagés	Impossible d'identifier les accès	Créer des comptes nominatifs
Justificatifs conservés trop longtemps	Conservation excessive	Définir des durées par finalité
Prestataires multiples	Contrats RGPD hétérogènes	Revue contractuelle systématique
Peu d'information aux salariés	Manque de transparence	Créer une notice claire et visible
Départs d'élus mal gérés	Accès résiduels	Checklist entrée/sortie des élus

Déclic

Les élus comprennent que le principal risque ne vient pas d'un manque de bonne volonté, mais de pratiques historiques devenues trop dispersées. Ils décident de traiter la conformité comme un chantier d'organisation.

2. Lancer un diagnostic simple et utile

Cartographier avant de corriger

Le référent RGPD organise un atelier de 90 minutes avec les élus concernés. L'objectif n'est pas d'établir immédiatement un registre parfait, mais de savoir quelles données existent, où elles sont stockées, qui y accède et pourquoi.

Question	Exemple de réponse	Action
Quelles données ?	Identité, coordonnées, enfants, quotient, justificatifs	Classer par sensibilité et nécessité
Pour quelle finalité ?	Attribuer une prestation ASC, informer, gérer une inscription	Supprimer les usages sans finalité claire
Où sont-elles ?	Logiciel ASC, drive, boîtes mail, postes locaux	Réduire les emplacements
Qui y accède ?	Élus ASC, secrétaire, prestataire	Limiter aux personnes nécessaires
Combien de temps ?	Durées variables ou inconnues	Fixer une durée par type de donnée
Quel prestataire ?	Billetterie, chèques cadeaux, plateforme loisirs	Vérifier les clauses de sous-traitance

3. Prioriser les actions à fort impact

Priorité	Action	Délai
1	Retirer les anciens accès et supprimer les comptes partagés	Immédiat
2	Sécuriser les fichiers contenant justificatifs ou données sensibles	Sous 10 jours
3	Définir les durées de conservation et lancer une première purge	Sous 30 jours
4	Mettre à jour les notices d'information et contrats prestataires	Sous 60 jours
5	Formaliser le registre et la revue trimestrielle	Sous 90 jours

4. Sécuriser les outils, accès et données ASC

Passer de la règle générale à des gestes concrets

Mesure	Mise en œuvre	Bénéfice
Comptes nominatifs	Un compte par élu ou gestionnaire	Traçabilité des accès
Authentification renforcée	MFA quand l'outil le permet	Réduction du risque de compromission
Habilitations par rôle	ASC, trésorerie, communication, administration	Accès au strict nécessaire
Stockage centralisé	Fin des copies locales permanentes	Moins de dispersion
Exports encadrés	Export temporaire, chiffrement, suppression après usage	Réduction des fuites
Durées formalisées	Calendrier de conservation et purge trimestrielle	Moins de données obsolètes
Prestataires revus	Clauses RGPD et sécurité vérifiées	Responsabilités clarifiées

Exemple ASC

Pour calculer une tranche d'aide, le CSE choisit de conserver le résultat utile plutôt que le justificatif complet lorsque celui-ci n'est plus nécessaire. Le principe appliqué est simple : ne garder que ce qui est utile au service rendu.

Résultat organisationnel

- Les élus savent qui a accès à quoi.
- Les fichiers sensibles ne circulent plus librement par mail.
- Les anciennes données sont supprimées selon un rythme défini.
- Le changement d'élu ou de prestataire déclenche automatiquement une revue des accès.

5. Former les élus et responsabiliser les usages

Une politique RGPD n'existe que si elle est appliquée

Le CSE met en place une sensibilisation courte, obligatoire pour les personnes ayant accès aux données. Le format privilégie les situations réelles plutôt qu'un cours juridique.

Situation	Réflexe attendu	Message clé
Réception d'un justificatif sensible	Déposer dans l'espace prévu, ne pas transférer	Éviter la duplication
Envoi d'un mail collectif	Utiliser le bon canal et vérifier les destinataires	Prévenir les divulgations
Départ d'un élu	Retirer immédiatement les accès	Fermer les droits sans délai
Nouvel outil ou prestataire	Vérifier sécurité et clauses RGPD avant déploiement	RGPD dès la conception
Demande d'un salarié	Orienter vers le référent et tracer la réponse	Respecter les droits

6. Communiquer avec transparence

Le CSE publie une information courte expliquant quelles données sont utilisées pour les ASC et les communications, pourquoi elles sont nécessaires, combien de temps elles sont conservées et comment exercer ses droits.

Message aux salariés

Le CSE protège les données qui lui sont confiées. Nous collectons uniquement les informations nécessaires aux prestations et communications proposées, limitons les accès, fixons des durées de conservation et réévaluons régulièrement nos pratiques.

- Éviter un discours alarmiste ou excessivement juridique.
- Dire ce qui a été amélioré et ce qui reste à faire.
- Donner un point de contact clair pour les questions liées aux données.

7. Mesurer les progrès et inscrire la démarche dans la durée

Quelques indicateurs suffisent pour piloter

KPI	Cible de pilotage	Fréquence
Traitements recensés et qualifiés	100 % des traitements identifiés	Trimestrielle
Accès revus	100 % des comptes actifs contrôlés	Trimestrielle
Comptes partagés	0 compte partagé	Mensuelle jusqu'à extinction
Prestataires avec clauses RGPD validées	100 % des prestataires critiques	Annuelle
Purge réalisée	100 % des catégories à échéance traitées	Trimestrielle
Élus sensibilisés	100 % des personnes habilitées	À chaque renouvellement
Incidents documentés	100 % des incidents ou quasi-incidents tracés	Au fil de l'eau

Rituel de gouvernance

Moment	Questions à traiter	Livrable
Trimestriel	Accès, incidents, purge, nouveaux outils	Tableau de bord RGPD
Annuel	Registre, prestataires, notices, durées	Revue de conformité
À chaque renouvellement	Comptes, habilitations, formation	Checklist passation
Avant nouveau service	Finalité, données, sécurité, contrat	Validation RGPD simplifiée

Enseignement

Le progrès ne vient pas d'une accumulation de procédures. Il vient d'un petit nombre de règles connues, appliquées et revues régulièrement. Le RGPD devient alors un standard de qualité du fonctionnement du CSE.

8. Checklists et plan d'action reproductible

Checklist : votre CSE est-il sur la bonne trajectoire ?

Question	Oui / Non	Action si non
Les traitements sont-ils recensés ?		Cartographier fichiers, outils et finalités.
Les accès sont-ils nominatifs et limités ?		Revoir les habilitations.
Les données inutiles sont-elles supprimées ?		Fixer des durées et lancer une purge.
Les prestataires sont-ils encadrés ?		Vérifier les clauses RGPD.
Les salariés sont-ils informés ?		Créer une notice simple et accessible.
Les élus sont-ils sensibilisés ?		Former les personnes habilitées.
Une procédure incident existe-t-elle ?		Créer un circuit d'alerte.
Une revue périodique est-elle planifiée ?		Inscrire un point trimestriel.

Plan d'action 30 jours

Jalon	Action	Livrable
J+5	Nommer un pilote et cartographier les traitements critiques	Diagnostic express
J+10	Traiter accès, comptes partagés et fichiers les plus sensibles	Quick wins sécurité
J+20	Définir durées, purges, notice et règles d'usage	Pack RGPD CSE
J+30	Former les élus et installer le tableau de bord	Politique RGPD opérationnelle

À retenir

Un CSE exemplaire en matière de RGPD n'est pas celui qui produit le plus de documents. C'est celui qui sait quelles données il traite, limite les accès, sécurise ses outils, informe les salariés et améliore régulièrement ses pratiques.

Références de travail

- RGPD : principes de minimisation, responsabilité, sécurité, registre et encadrement des sous-traitants.
- CNIL : registre des traitements, sécurité des données, gestion des violations, droits des personnes.
- En cas de doute ou d'incident significatif, solliciter l'appui juridique CFE-CGC Mutualité / ALINEA ou un conseil spécialisé.

CFE-CGC Mutualité | Réflexe élu : cartographier - sécuriser - informer - réviser