

GUIDE PRATIQUE

Les risques encourus en cas de non-respect du RGPD par un CSE

Prévenir les sanctions, protéger les salariés et sécuriser le fonctionnement de l'instance

Finalité du guide	Donner aux élus une lecture concrète des risques juridiques, financiers, opérationnels et réputationnels liés à une mauvaise gestion des données personnelles.
Public cible	Élus du CSE, secrétaire, trésorier, commissions, gestionnaires ASC, référent RGPD, prestataires et personnes habilitées.
Usage recommandé	Audit RGPD, revue annuelle, changement de logiciel ASC, incident de sécurité, renouvellement des élus, contractualisation d'un prestataire.
Résultat attendu	Identifier rapidement les écarts, les prioriser selon le risque et mettre en œuvre un plan de conformité traçable.

Message central

Le risque RGPD ne se limite pas à une amende. Un manquement peut entraîner injonctions, limitation d'un traitement, atteinte à la confiance, demandes d'indemnisation et, dans certains cas, sanctions pénales. La meilleure défense reste une conformité démontrable et proportionnée.

- Le CSE doit savoir quels fichiers il détient, pourquoi, pour combien de temps et avec quels accès.
- Une violation de données doit être traitée comme un incident : contenir, documenter, évaluer, notifier si nécessaire.
- Les sanctions administratives sont proportionnées à la gravité du manquement ; le plafond de 4 % du chiffre d'affaires concerne le cas des entreprises.
- La responsabilité personnelle d'un élu n'est pas automatique : elle dépend de son comportement et du fondement juridique applicable.

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

Sommaire

- 1. Comprendre les catégories de risques**
- 2. Connaître les pouvoirs et sanctions de la CNIL**
- 3. Identifier les manquements les plus exposés**
- 4. Réagir à une violation de données**
- 5. Clarifier la responsabilité du CSE et des élus**
- 6. Conduire un audit RGPD simple**
- 7. Piloter un plan de mise en conformité**
- 8. Checklists, KPI et plan d'action 30 jours**

Principe directeur

Le niveau de risque dépend de la nature des données, du nombre de salariés concernés, de la durée du manquement, des mesures de sécurité, de la coopération et des conséquences pour les personnes. Un CSE doit donc raisonner en criticité plutôt qu'en conformité purement documentaire.

1. Comprendre les catégories de risques

Un même incident peut produire plusieurs conséquences

Type de risque	Exemple	Impact possible
Juridique	Base légale absente, défaut d'information, durée excessive	Mise en conformité imposée, limitation du traitement, contentieux
Financier	Sanction administrative, frais d'expertise ou de remédiation	Impact sur le budget du CSE
Opérationnel	Compte compromis, perte d'un fichier ASC	Interruption du service, reconstitution des données
Réputationnel	Divulgaration de situations familiales ou de santé	Perte de confiance des salariés
Humain	Atteinte à la vie privée, exposition d'une situation sensible	Préjudice pour la personne concernée
Gouvernance	Accès non retirés après départ d'un élu	Responsabilités floues, répétition des incidents

Matrice de criticité

Criticité	Exemples	Réponse
Faible	Notice d'information à actualiser, fichier ancien sans données sensibles	Correction planifiée
Moyenne	Durée de conservation non maîtrisée, habilitations trop larges	Action sous 30 jours
Élevée	Données sensibles exposées, prestataire non encadré, droits non traités	Remédiation immédiate
Critique	Fuite active, accès externe, volume important, risque élevé pour les personnes	Cellule incident + analyse notification CNIL/personnes

Réflexe élu

Ne pas attendre un contrôle pour agir : les plaintes de salariés, un changement de prestataire ou une fuite de données sont souvent les déclencheurs d'un examen approfondi.

2. Pouvoirs et sanctions de la CNIL

Une palette de mesures graduées

La CNIL peut intervenir après une plainte, un contrôle ou la connaissance d'un incident. Elle dispose de pouvoirs correctifs et répressifs qui s'adaptent à la gravité et au contexte.

Mesure possible	Conséquence pour le CSE
Rappel à l'ordre	Constat formel du manquement et obligation de correction
Injonction de mise en conformité	Plan d'action imposé, éventuellement sous astreinte
Limitation ou suspension d'un traitement	Arrêt ou restriction d'un service utilisant les données
Satisfaction des droits des personnes	Obligation de répondre à une demande d'accès, effacement, opposition, etc.
Amende administrative	Sanction pécuniaire proportionnée, pouvant être rendue publique en procédure ordinaire

Plafonds : bien lire la règle

Le RGPD prévoit, pour les manquements les plus graves, un plafond pouvant atteindre 20 millions d'euros. Le plafond alternatif de 4 % du chiffre d'affaires annuel mondial vise le cas d'une entreprise. En pratique, le montant d'une sanction doit rester effectif, proportionné et dissuasif et tient compte du cas concret.

Au-delà de la CNIL

- Une personne ayant subi un dommage matériel ou moral peut demander réparation sur le fondement du RGPD.
- Le droit français prévoit aussi certaines infractions pénales liées aux traitements de données, notamment en matière de sécurité ou de notification des violations.
- Une décision publique de la CNIL peut avoir un impact réputationnel supérieur au montant de l'amende elle-même.

3. Les manquements les plus exposés

Les risques viennent souvent d'usages banalisés

Manquement	Exemple terrain	Action de prévention
Minimisation insuffisante	Conserver un avis d'imposition complet pour une simple tranche ASC	Ne stocker que l'information utile
Accès excessifs	Tous les élus voient les dossiers individuels	Habilitations par rôle
Durée indéfinie	Archives ASC conservées sans échéance	Politique de conservation + purge
Sécurité faible	Compte partagé, mot de passe commun, export local	Comptes nominatifs, MFA, stockage sécurisé
Information absente	Formulaire sans notice RGPD	Mention d'information standardisée
Prestataire mal encadré	Billetterie sans clause de sous-traitance	Contrat article 28 et revue annuelle
Données sensibles mal protégées	Justificatif médical accessible largement	Accès strict, durée courte, nécessité démontrée

Signaux d'alerte à traiter immédiatement

- Un fichier Excel circule par messagerie avec des données familiales ou financières.
- Un ancien élu ou prestataire conserve encore un accès.
- Personne ne sait expliquer pourquoi certaines pièces sont conservées.
- Une demande d'accès ou d'effacement reste sans réponse.
- Un incident a eu lieu mais n'a pas été documenté.

Règle de méthode

Le bon réflexe n'est pas « avons-nous un document RGPD ? », mais « pouvons-nous démontrer que le traitement est nécessaire, maîtrisé et sécurisé ? ».

4. Réagir à une violation de données

Une violation = perte, destruction, altération, divulgation ou accès non autorisé

Étape	Action	Délai / vigilance
1. Contenir	Bloquer accès, lien, compte ou export compromis	Immédiat
2. Documenter	Nature, volume, personnes, durée, cause, destinataires	Dès découverte
3. Évaluer	Risque pour les droits et libertés des personnes	Sans délai
4. Décider	Notification CNIL si le risque le justifie	En principe sous 72 h à compter de la connaissance
5. Informer	Informar les personnes si le risque est élevé	Sans délai indu
6. Corriger	Mot de passe, habilitations, procédure, contrat, formation	Plan d'action tracé

À ne pas faire

Supprimer les traces, minimiser l'incident, attendre de connaître toutes les conséquences avant de l'enregistrer, ou prévenir largement sans maîtriser les faits. La transparence doit être organisée, factuelle et proportionnée.

5. Responsabilité du CSE et des élus

Lorsque le CSE détermine les finalités et moyens d'un traitement, la responsabilité RGPD pèse en principe sur l'organisme responsable du traitement. La responsabilité personnelle d'un élu n'est donc pas automatique. Elle peut toutefois être recherchée sur d'autres fondements lorsque son comportement personnel constitue une faute ou une infraction caractérisée.

- Éviter de présenter une « négligence grave » comme un régime automatique de responsabilité RGPD des élus.
- Formaliser qui administre les outils, qui autorise les accès et qui gère les incidents.
- Former les élus et bénévoles à la confidentialité et aux règles de sécurité.

6. Conduire un audit RGPD simple

Un audit orienté risques, en 6 blocs

Bloc	Questions de contrôle	Preuve attendue
Traitements	Tous les fichiers et outils sont-ils recensés ?	Registre / cartographie
Bases et information	Finalité, base, notice et droits sont-ils maîtrisés ?	Mentions et formulaires
Accès	Qui peut voir quoi ? Les départs sont-ils traités ?	Matrice habilitations
Conservation	Les données obsolètes sont-elles supprimées ?	Politique + journal de purge
Prestataires	Les contrats encadrent-ils la protection des données ?	Annexe RGPD / DPA
Incidents	Existe-t-il un circuit d'alerte et un registre ?	Procédure + registre incidents

KPI de pilotage

- % de traitements recensés et qualifiés.
- % de comptes avec MFA quand disponible.
- % d'habilitations revues sur les 3 derniers mois.
- % de prestataires avec clauses RGPD validées.
- Nombre de données/fichiers supprimés après revue.
- Nombre d'incidents et délai moyen de qualification.

Gouvernance recommandée

Un référent RGPD du CSE coordonne le suivi, mais chaque élu reste responsable du respect des règles dans ses usages. Une revue trimestrielle courte vaut mieux qu'un audit lourd une fois tous les trois ans.

7. Checklists et plan d'action

Checklist de mise en conformité prioritaire

Question	Oui / Non	Action si non
Le registre est-il à jour ?		Recenser fichiers, finalités et responsables.
Les données sensibles sont-elles identifiées ?		Limiter les accès et documenter la nécessité.
Les comptes sont-ils nominatifs ?		Supprimer les comptes partagés.
Les anciens accès sont-ils retirés ?		Revue immédiate des habilitations.
Les durées de conservation sont-elles fixées ?		Créer un calendrier de purge.
Les prestataires sont-ils encadrés ?		Vérifier contrat et sécurité.
Une procédure incident existe-t-elle ?		Créer un circuit d'alerte et un registre.
Les élus sont-ils formés ?		Sensibilisation 45 minutes + rappel annuel.

Plan d'action 30 jours

Jalon	Action	Livrable
J+5	Recenser les traitements et accès critiques	Cartographie express
J+10	Traiter les risques critiques : accès, données sensibles, exports	Quick wins sécurisation
J+20	Mettre à jour notices, contrats et durées	Pack conformité
J+30	Valider gouvernance, procédure incident et KPI	Tableau de bord RGPD CSE

À retenir

Le coût principal d'un manquement RGPD peut être juridique, financier, opérationnel et réputationnel. La conformité la plus efficace repose sur quatre réflexes : minimiser, sécuriser, documenter et réviser régulièrement.

Références de travail

- RGPD : art. 5, 24, 28, 30, 32 à 34, 82 et 83.
- CNIL : définition du responsable de traitement ; pouvoirs et sanctions ; sécurité ; violations de données.
- Code pénal / loi Informatique et Libertés : infractions applicables selon les faits. Vérifier avec ALINEA ou un conseil spécialisé en cas d'incident ou de contentieux.

CFE-CGC Mutualité | Réflexe élu : identifier - contenir - documenter - corriger