SONDAGE CSE

L'institut de sondage des représentants du personnel

my data partner

Élus du CSE : comprendre vos obligations RGPD

et agir concrètement, avec méthode.

Sous la direction de nos avocates partenaires
Maître Nacima Lamalchi-Elkilani
Maître Sabine Abecassis
Avocates au Barreau de Paris & DPO certifiées.

www.sondage-cse.fr

« Votre CSE peut atteindre un niveau de conformité solide en six à neuf mois… »

En France, plus de 35 000 CSE, COS et CASI manipulent chaque jour des données personnelles souvent sensibles : revenus pour le quotient familial, composition familiale, situations de handicap, réponses aux enquêtes QVCT.

Le problème : la majorité des élus ignorent que leur CSE est soumis au RGPD en qualité de responsable de traitement, distinct de l'employeur. Beaucoup d'autres se croient en conformité sur la base d'idées reçues.

Ce guide, conçu pour les élus non-juristes, vous donne l'essentiel : vos obligations, vos risques, les actions à lancer. Sans jargon. Sans liste interminable de textes.

Bonne nouvelle : avec une méthode claire, votre CSE peut atteindre un niveau de conformité solide en six à neuf mois.

Nacima Lamalchi-Elkilani, avocate au Barreau de Paris, co-fondatrice de MyDataPartner

3 choses que tout élu du CSE doit savoir

1 | **Votre CSE est une entité juridique autonome dès 50 salariés (art. L. 2315-23 du Code du travail). Ses obligations RGPD sont distinctes de celles de l'entreprise.**

2 | **Le DPO de l'entreprise ne couvre pas votre CSE. Sauf accord écrit explicite, c'est le CSE, et son secrétaire en premier rang, qui répond de la conformité.**

3 | **La CNIL peut sanctionner directement votre CSE. Et les salariés peuvent engager la responsabilité de l'instance, voire des élus eux-mêmes.**

1 Ce que vous devez savoir

Votre CSE est un responsable de traitement

Le RGPD s'applique à toute entité qui décide pourquoi et comment elle collecte des données personnelles.
Votre CSE remplit cette définition dès qu'il gère les ASC, organise un sondage ou tient un fichier de bénéficiaires.

Conséquence juridique : il a le statut de « responsable de traitement » (art. 4.7 du RGPD).
Et cette qualité ne se partage pas avec l'employeur.

Concrètement, votre CSE doit :

- tenir son propre registre des traitements, distinct de celui de l'entreprise ;
- informer les salariés que c'est lui qui collecte leurs données, pas l'employeur ;
- signer ses propres contrats avec ses prestataires et en suivre l'exécution ;
- définir et respecter des durées de conservation ;
- répondre lui-même aux demandes des salariés (accès, rectification, suppression) ;
- déclarer les incidents de sécurité.

Les 4 risques concrets pour les élus

Risque 1 : sanction CNIL.
Mise en demeure, injonction, amendes (art. 83 RGPD). Pour un CSE, l'amende est calibrée à la taille de la structure mais peut atteindre six chiffres.

Risque 2 : action des salariés.
Tout salarié dont les données ont été mal traitées peut demander réparation devant les tribunaux (art. 82 RGPD). Position délicate pour une instance censée représenter les salariés.

Risque 3 : sanctions pénales.
Jusqu'à 5 ans de prison et 300 000 € d'amende pour les personnes physiques (art. 226-16 et suivants du Code pénal).

Risque 4 : perte de crédibilité.
Après un incident, les salariés ne répondent plus aux sondages, les expertises sont contestées, le CSE perd son levier d'action.

La première sanction d'un CSE : CNIL, 27 décembre 2023

Un CSE est condamné à 10 000 € d'amende lors d'un simple contrôle simplifié. Il avait pourtant désigné un DPO.

Le contrôle a révélé : registre des traitements absent, mentions d'information lacunaires, contrat de sous-traitance non conforme.

Et en février 2026 : des dizaines de CSE victimes d'une fuite de données via la plateforme de leur prestataire ; en mars, violation confirmée au CSE Scalian via un applicatif tiers.

À retenir : désigner un DPO ne suffit pas. Et le CSE reste responsable même si son sous-traitant est défaillant.

② Vos obligations RGPD par interlocuteur

1 | Avec les salariés et leurs familles : la plus volumineuse en données, revenus, composition familiale, parfois handicap (donnée de santé, art. 9 RGPD).

Les réflexes :

- informer avant de collecter (art. 13 et 14) ;
- ne collecter que le strict nécessaire ;
- consentement explicite et accès restreint pour les données sensibles ;
- durées de conservation définies et appliquées ;
- réponse aux demandes des salariés sous un mois (art. 12).

En pratique : le quotient familial

Ne demandez pas l'avis d'imposition complet. La première page, avec le seul revenu fiscal de référence, suffit ; autres informations masquées, archivage à date définie. Vos salariés le remarquent, et la confiance se renforce.

2 | Avec les élus du CSE : la plus souvent oubliée

Les élus sont eux-mêmes des personnes concernées : mandats, heures de délégation, appartenance syndicale (donnée sensible, art. 9).

Les réflexes :

- information en début de mandat ;
- matrice d'habilitation par fonction, car tous les élus n'ont pas vocation à tout voir ;
- engagement de confidentialité signé ;
- révocation immédiate des accès en fin de mandat ;
- aucune donnée nominative dans les groupes WhatsApp personnels.

② Vos obligations RGPD par interlocuteur

3 | Avec les prestataires : la plus contractualisée

Plateformes ASC, billetterie, instituts de sondage, hébergeurs : le RGPD les qualifie de « sous-traitants » (art. 28).

Les réflexes :

- sélectionner sur garanties vérifiées ;
- signer un contrat conforme à l'article 28 ;
- connaître et autoriser la chaîne complète des sous-sous-traitants ;
- vérifier la conformité au moins une fois par an.

Idée reçue fréquente

« Notre prestataire est dans le métier depuis 15 ans, il gère le RGPD pour nous. On est tranquilles. »

FAUX.
Le prestataire gère ses obligations propres. Le CSE, responsable de traitement, doit l'avoir choisi avec discernement, encadré par contrat et suivi dans la durée.
À défaut, le simple transfert de données au prestataire constitue une faute.

4 | Avec l'employeur : la plus délicate

Le principe : l'employeur est un tiers aux traitements du CSE. Il n'accède ni au fichier des bénéficiaires des ASC, n aux revenus déclarés, ni aux réponses individuelles de vos enquêtes. À encadrer par écrit : la transmission de la liste des salariés (périmètre limité au nécessaire, canal sécurisé) et les élections professionnelles.

Ce que le CSE peut transmettre à l'employeur

AUTORISÉ :
- résultats agrégés et anonymisés (avec effectifs suffisants pour empêcher la réidentification) ;
- PV de réunion de CSE.

INTERDIT :
- réponses brutes individuelles à une enquête ; copie nominative du fichier des bénéficiaires des ASC ;
- dossiers individuels de réclamation.

5 | Avec les autres CSE du groupe :

la plus sous-estimée CSEE, CSEC, CSE de groupe : des entités distinctes, sans accès de droit aux données des autres.
Qualifiez chaque transfert (art. 26 ou 28), anonymisez les remontées au CSEC, harmonisez par une charte inter-CSE.
Bonne pratique : un DPO externalisé mutualisé, indépendant de l'employeur.

3 Le cas des enquêtes CSE

Les enquêtes QVCT, RPS et baromètres touchent souvent à la santé (données sensibles), mobilisent un prestataire externe (sous-traitance), intéressent l'employeur (partage à encadrer) et peuvent permettre de réidentifier des salariés.

Les 7 réflexes RGPD

1. TRANSPARENCE :
mention d'information diffusée avant toute collecte (art. 13).

2. FINALITÉ DÉFINIE :
une enquête QVCT sert à la QVCT, à rien d'autre (art. 5.1.b).

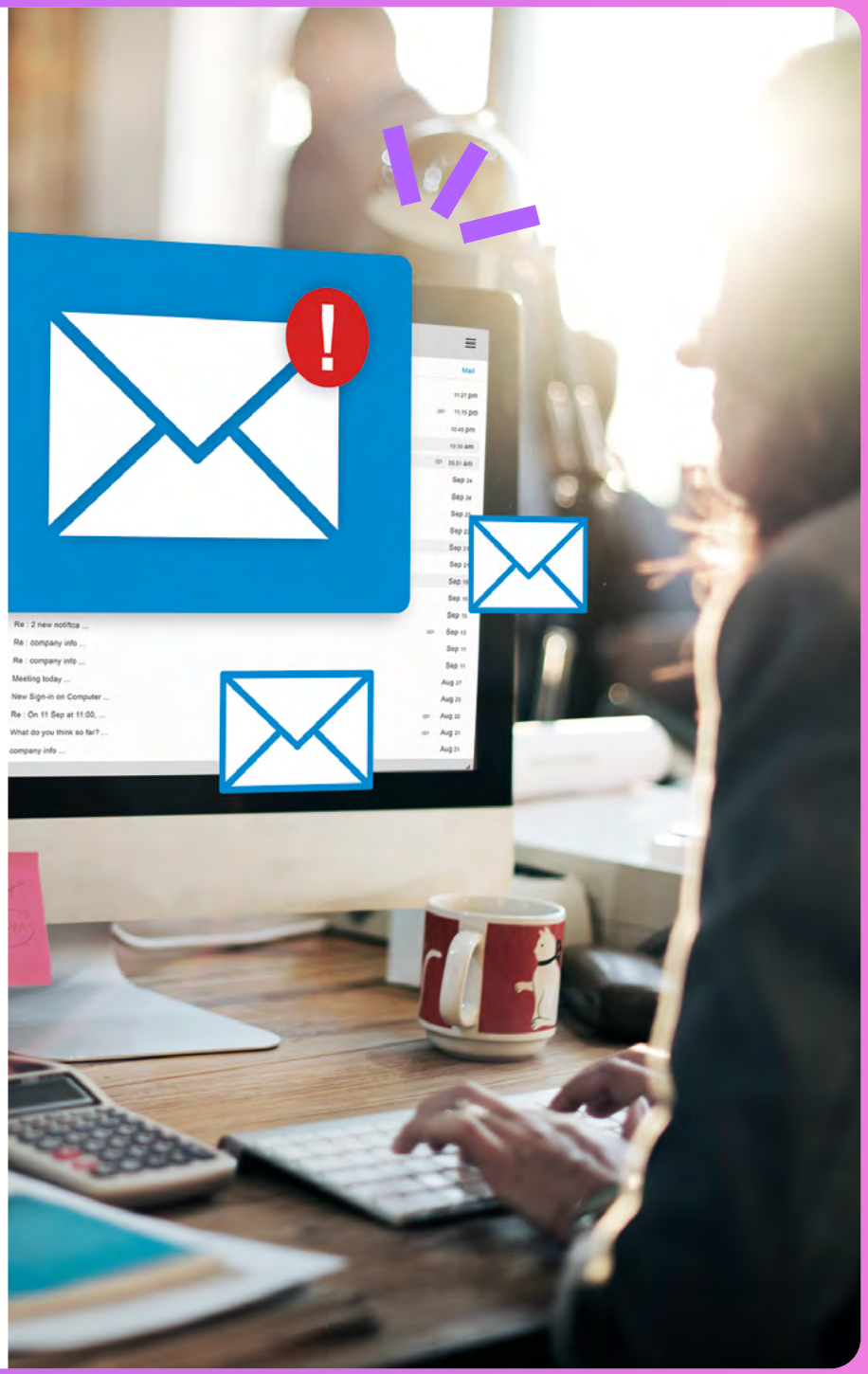
3. MINIMISATION :
une tranche d'âge plutôt que l'âge exact, un identifiant aléatoire plutôt qu'un nom (art. 5.1.c).

4. DONNÉES SENSIBLES :
consentement explicite et sécurité renforcée dès que l'enquête touche à la santé mentale (art. 9).

5. SÉCURITÉ :
chiffrement, accès restreints ; aucun fichier Excel de répondants envoyé par e-mail (art. 32).

6. DURÉE LIMITÉE :
réponses brutes supprimées 3 à 6 mois après la restitution ; résultats agrégés et anonymisés conservés librement (art. 5.1.e).

7. PARTAGE ENCADRÉ :
contrat art. 28 avec le prestataire ; résultats agrégés uniquement vers l'employeur.



3 Le cas des enquêtes CSE (suite)

Les 3 pièges à éviter

Piège 1 :
la liste des salariés envoyée par e-mail

Pièce jointe Excel non chiffrée, aucune traçabilité, exposition directe à une violation. Préférez l'espace de dépôt sécurisé du prestataire ; à défaut, fichier chiffré et mot de passe transmis par un autre canal.

Piège 2 :
le faux anonymat.

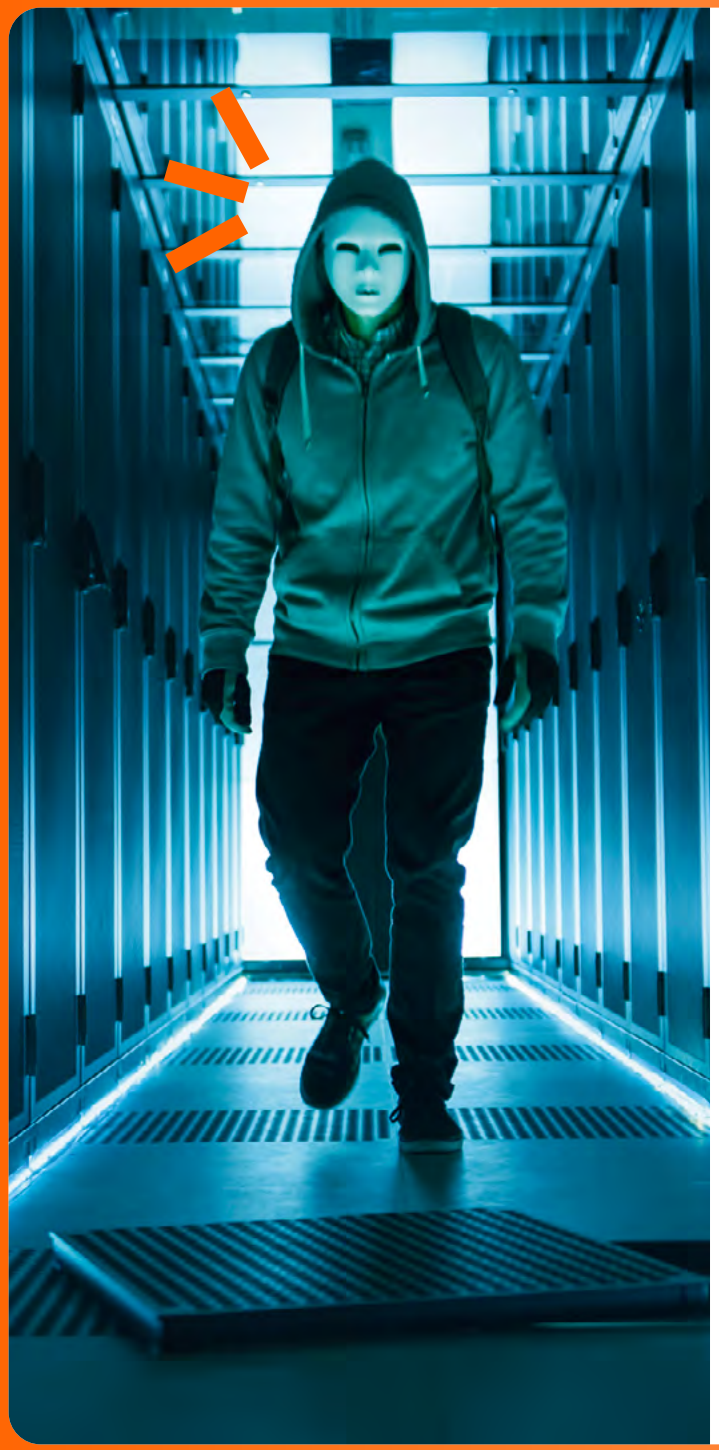
« Le matricule entreprise, c'est anonyme. »
Faux : c'est de la pseudonymisation. Générez un identifiant aléatoire ; la table de correspondance reste chez le seul prestataire et est détruite à la clôture, avec certificat.

Piège 3 :
les données brutes qui dorment.

Définissez une durée de conservation explicite, inscrivez-la au registre et exigez un certificat de destruction du prestataire.

Le bon arbitrage

Une enquête conforme est une enquête à laquelle les salariés répondent en confiance : meilleur taux de participation, résultats plus fiables, crédibilité renforcée du CSE. La conformité n'est pas une contrainte bureaucratique, c'est un facteur de qualité méthodologique.



4 En cas de violation de données : les 5 premiers gestes

Les enquêtes QVCT, RPS et baromètres touchent souvent à la santé (données sensibles), mobilisent un prestataire externe (sous-traitance), intéressent l'employeur (partage à encadrer) et peuvent permettre de réidentifier des salariés.

Geste 1 : qualifier.
S'agit-il d'une violation de confidentialité (données divulguées), d'intégrité (données altérées) ou de disponibilité (données perdues ou inaccessibles) ? Notez l'heure et la manière dont vous en avez pris connaissance : le délai court à partir de là.

Geste 2 : contenir et documenter.
Stoppez la fuite (révocation d'accès, retrait du fichier), rassemblez les faits : nature des données, personnes concernées, volume, conséquences possibles. Consignez tout par écrit.

Geste 3 : apprécier le risque, au cas par cas.
C'est le geste décisif. La notification à la CNIL n'est pas automatique : elle s'impose sauf si la violation n'est pas susceptible d'engendrer un risque pour les droits et libertés des personnes, notamment leur vie privée (art. 33 RGPD).

Cette appréciation se fait au cas par cas, selon la nature et la sensibilité des données, leur volume, les personnes touchées et les conséquences possibles pour elles.
Elle doit être documentée : c'est elle que la CNIL examinera.

Geste 4 : notifier la CNIL sous 72 heures si le risque est caractérisé.
Le délai court à compter de la prise de connaissance de la violation. En cas de doute sur l'appréciation du risque, faites-vous accompagner : ne pas notifier à tort et notifier inutilement ont l'un et l'autre un coût.

Geste 5 : informer les personnes concernées si le risque est élevé (art. 34).
Dans les meilleurs délais, en termes clairs et simples : nature de la violation, conséquences probables, mesures prises, point de contact.

Dans tous les cas : le registre des violations

Inscrivez la violation au registre des violations, même si vous concluez qu'elle n'a pas à être notifiée (art. 33.5). Ce registre documente votre appréciation du risque et prouve votre diligence en cas de contrôle.

A propos de MyDataPartner

MyDataPartner est la LegalTech dédiée à la conformité RGPD et IA des CSE. Notre mission : rendre la conformité numérique accessible aux élus non-juristes, sans jargon, sans paperasse inutile, avec des outils opérationnels et un accompagnement humain par nos avocates partenaires.

L'équipe est portée par ses deux fondatrices, Maître Nacima Lamalchi-Elkilani et Maître Sabine Abecassis, avocates au Barreau de Paris, expertes en droit du numérique et conformité (RGPD, AI Act, NIS2, DORA), avec plus de 20 ans d'expérience chacune auprès des entreprises et des CSE.

2 façons simples et gratuites de démarrer

1. RGPD Score

Évaluez votre situation en 5 minutes et recevez une analyse personnalisée par e-mail.
> qmoa8rm4la6.typeform.com/to/mBdwn1LK

2. Audit de 30 minutes

Un échange en visio avec l'une de nos avocates partenaires pour comprendre votre situation et identifier vos 3 priorités.
> mydatapartner.com/avis-conseil/

contact@mydatapartner.com | 01.56.59.42.89 | www.mydatapartner.com
64 rue de Miromesnil, 75008 Paris