



CNIL : questions-réponses élections professionnelles et données personnelles

➤ **Liste électorale**

- Quelles mentions l'employeur peut-il faire figurer sur la liste électorale concernant ses agents/salariés ?

Les mentions devant figurer sur la liste électorale devraient être précisées entre l'employeur et les organisations syndicales dans l'accord préélectoral.

La Cour de cassation a précisé que doivent figurer sur la liste électorale les seules informations suivantes :

- les nom et prénom,
- l'âge,
- l'appartenance à l'entreprise,
- l'ancienneté (qui doit être de trois mois au minimum).

Ces mentions déterminent la qualité d'électeur et permettent le contrôle de la régularité de la liste électorale.

Elles permettent aussi, plus généralement, de l'organisation des opérations électorales qui en découlent.

Au contraire, des informations comme l'adresse du domicile n'ont pas à figurer sur la liste électorale, sauf dans des cas très particuliers (p. ex. : salariés exerçant à domicile).

La réglementation ne prévoyant pas les mentions à faire figurer sur la liste électorale, la CNIL considère qu'en vertu du principe de minimisation des données, cette dernière ne devrait pas indiquer d'autres informations que celles permettant de vérifier que l'agent répond aux critères susmentionnés.

➤ **Qualification des acteurs**

- Quel est le statut des centres de gestion assurant l'organisation des élections professionnelles pour le compte des collectivités territoriales ?

Les centres de gestion sont, en principe, responsables des traitements de données personnelles mis en œuvre aux fins d'organiser les élections professionnelles, au sens de l'article 4-7) du RGPD.

Les centres de gestions assurent le fonctionnement des commissions administratives paritaires ainsi que le fonctionnement des comités sociaux et territoriaux, pour l'ensemble des agents des collectivités territoriales et établissements publics affiliés.

Par conséquent, les collectivités territoriales et les établissements publics concernés n'interviennent pas dans l'organisation des élections professionnelles :

- ils ne donnent aucune instruction aux centres de gestion pour définir le dispositif de vote à déployer,
- ils ne déterminent pas les caractéristiques essentielles des traitements de données personnelles nécessaires dans ce contexte (notamment à quoi sert le traitement, ce qui en est attendu, la nature des données personnelles collectées, les mesures de sécurité, etc.),
- ils n'exercent sur ces traitements aucune influence et ne disposent d'aucun pouvoir décisionnel.

En revanche, il appartient aux centres de gestion de choisir ou non de recourir au vote électronique par Internet et s'il en constitue le seul mode d'expression des suffrages.

En cas de vote électronique, les centres de gestion en détermineront les modalités d'organisation : choix du prestataire de la solution de vote électronique, détermination de la nature des données à collecter et des modalités d'authentification des électeurs, procédure de réassort (réinitialisation des moyens d'authentification, par exemple en cas de perte ou d'oubli), etc.

- Le prestataire de solution de vote par correspondance électronique mettant en œuvre les élections professionnelles pour le compte de l'organisateur de l'élection est-il sous-traitant ?

Généralement oui.

Le prestataire de solution de vote électronique est, en principe, sous-traitant au sens du RGPD, dans la mesure où il traite des données personnelles des électeurs pour le compte et sur instruction de l'organisateur de l'élection (p. ex. : employeur, centre de gestion).

La nature du service effectué par le prestataire de solution de vote électronique, auquel fait appel l'organisateur de l'élection, permet de donner des indices pour retenir cette qualification.

En effet, ce prestataire traite des données personnelles pour répondre exclusivement aux besoins de l'organisateur de l'élection tenu d'assurer le renouvellement des représentants du personnel.

Le traitement est effectué par le prestataire à la demande de l'organisateur de l'élection qui en fixe les caractéristiques essentielles (finalité, nature des données collectées, durée de conservation des données, mesures de sécurité, etc.).

Les données personnelles des électeurs (adresses email professionnelles, coordonnées postales, matricule agent/salarié non public etc.) sont transmises au prestataire par l'organisme responsable de l'organisation de l'élection.

En cas de recours à un sous-traitant, l'organisateur de l'élection, en tant que responsable de traitement, doit respecter toutes les obligations du RGPD, en particulier l'information des personnes (voir question n° 14) et de formaliser la relation de sous-traitance

- Comment qualifier, au sens du RGPD, l'expert indépendant qui atteste de la sécurité de la solution de vote électronique et du bon déroulement du processus électoral ?

Le cadre d'intervention de l'expert étant variable, sa qualification doit être analysée au cas par cas.

L'expert indépendant ne traite généralement pas de données personnelles lors de son expertise de la solution de vote électronique et du processus électoral.

Dans le cas où l'expert aurait accès à ces données de manière purement accessoire et très limité dans la pratique, il pourrait être considéré qu'il n'opère pas de traitement de données personnelles.

Ainsi, l'expert ne serait ni sous-traitant ni responsable de traitement.

Lorsque l'expert traite des données personnelles, l'analyse peut être guidée par les lignes directrices du Comité européen de la protection des données sur les notions de responsable de traitement et de sous-traitant, qui livrent un certain nombre de précisions et d'exemples ainsi qu'un arbre de décision.

Si votre situation correspond aux critères ci-dessous (qui composent un faisceau d'indices), il est très probable que l'expert soit sous-traitant :

- l'expert est mandaté pour effectuer un traitement de données spécifique et a reçu des instructions détaillées en la matière,
- l'expert ne pourra pas traiter les données auxquelles il a accès pour d'autres finalités que celles indiquées par le responsable de traitement (c'est-à-dire pour une finalité qui lui est propre),
- l'expert ne tirera aucun bénéfice du traitement autre que la simple rémunération de ses services et ne réexploite pas les données pour son compte,
- le responsable de traitement exerce un contrôle des activités de traitement de l'expert afin de s'assurer que celui-ci respecte les instructions et les stipulations contractuelles.

Si la plupart des critères ci-dessus ne correspondent pas à votre situation, le faisceau d'indices pourrait plutôt pencher vers la qualification de l'expert en tant que responsable de traitement.

➤ **Gestion de la conformité et protection des droits des personnes concernées**

- Quels documents de la CNIL faut-il prendre en compte dans l'organisation d'un scrutin ayant recours au vote par correspondance électronique ?

Le vote électronique a fait l'objet d'une recommandation de la part de la CNIL le 25 avril 2019.

Celle-ci est entrée en vigueur le 21 juin 2020.

Cette recommandation est complétée par la fiche pratique Sécurité des systèmes de vote par internet : la CNIL actualise sa recommandation de 2010 publiée sur le site de la CNIL.

Cette recommandation présente aux responsables de traitement souhaitant recourir à un tel système de vote une approche pragmatique, fournissant les objectifs de sécurité à atteindre en fonction du niveau de risque.

La recommandation s'accompagne d'une fiche pratique qui présente une méthodologie en deux temps :

- une grille d'analyse pour déterminer le niveau de sécurité que le système de vote par correspondance électronique doit respecter (ces questions portent notamment sur le nombre d'électeurs, sur l'utilisation d'autres modalités de vote ou encore sur le pouvoir décisionnel des personnes élues),
- des objectifs de sécurité avec des exemples de moyens minimaux à mettre en œuvre pour atteindre ces objectifs.

En pratique, la CNIL identifie généralement un risque de niveau 2 (intermédiaire) pour la plupart des élections des représentants du personnel aux instances représentatives, sauf cas particulier tels qu'une élection à grande échelle se déroulant dans un organisme important et dans un cadre conflictuel, qui relèvent du niveau 3 (le plus élevé).

Une fois le niveau de risque établi, l'organisateur de l'élection (qui est également responsable du traitement) peut déterminer les objectifs de sécurité que le dispositif de vote électronique doit atteindre.

Dans le cadre des élections professionnelles, tout dispositif de vote par correspondance électronique devrait notamment inclure, à la manière de ce qui se fait pour le vote papier, un contrôle automatique de l'intégrité du système, de l'urne et de la liste d'émargement, ainsi qu'un dispositif d'authentification des électeurs permettant de s'assurer que les risques majeurs et mineurs liés à une usurpation d'identité sont réduits de manière significative.

- Vote par correspondance électronique : faut-il procéder à une formalité préalable auprès de la CNIL ?

Non.

Aucune formalité particulière ne doit être réalisée auprès de la CNIL en cas de recours au vote par correspondance électronique aux élections des représentants du personnel au sein des instances représentatives.

En revanche, l'organisateur de l'élection, qui agit en qualité de responsable de traitement, doit à ce titre respecter ses obligations au regard du RGPD :

- la réalisation d'une analyse d'impact relative à la protection des données (AIPD),
- l'inscription préalable du traitement au registre des activités de traitement,
- l'information des personnes, notamment sur le déroulement des opérations de vote et sur le fonctionnement du système de vote électronique (en fournissant une notice, par exemple),
- l'encadrement du contrat de sous-traitance s'il est fait appel à un prestataire extérieur, etc.

Lorsque l'AIPD réalisée préalablement à l'organisation du vote électronique indique que le traitement de données personnelles utilisé présente un risque résiduel élevé pour les droits et libertés des électeurs et s'il ne prend pas de mesures pour atténuer ce risque, l'organisateur de l'élection doit consulter la CNIL (art. 36 du RGPD).

- Comment informer les électeurs concernés de l'utilisation de leurs données personnelles ?
 - Qui doit informer ?

L'organisateur de l'élection est responsable de traitement : il doit donc informer les personnes concernées.

Il peut le faire lui-même ou confier cette opération à son sous-traitant, en contrôlant que l'information soit délivrée conformément à ce que prévoit le RGPD.

En cas de vote par correspondance électronique, l'organisateur de l'élection informe individuellement les agents/salariés de la transmission de certaines de leurs données personnelles au prestataire de solution de vote.

Il peut également déléguer, en la contrôlant, cette information au prestataire.

Celui-ci pourra ensuite organiser le scrutin.

- Comment informer ?

Le responsable de l'élection doit définir les mesures appropriées afin de fournir une information complète, aisément accessible et de nature à faciliter l'exercice des droits des électeurs dont les données sont collectées.

Lorsque le responsable dispose d'un moyen simple lui permettant d'atteindre directement l'électeur (p. ex. : adresse e-mail professionnelle, information transmise au moment de la remise de la fiche de paie), il convient de privilégier ces supports de communication.

L'information rendue accessible dans un lieu de passage ne peut généralement intervenir qu'en rappel ou en complément d'une information exhaustive et directement adressée à la personne.

- Quand informer ?

L'information doit être délivrée aux salariés/agents concernés au moment de la collecte de leurs données personnelles, et peut être renouvelée à tout moment, lorsque cela est jugé opportun, afin notamment de faciliter l'exercice des droits des personnes.

Par exemple, l'employeur informe l'agent/salarié à son embauche de la collecte de son IBAN à des fins de gestion de paie et, le cas échéant, d'une partie de celui-ci à des fins d'authentification dans le cadre du vote électronique.

Une nouvelle information peut être délivrée à ce dernier peu de temps avant l'utilisation effective de cette donnée pour les élections professionnelles, afin de lui rappeler la mise en œuvre du traitement ou lorsque cela n'a pas été réalisé au moment de l'embauche.

- **Solution de vote par correspondance électronique et mesures de sécurité**

- L'organisateur de l'élection ou son prestataire de solution de vote peuvent-ils envoyer au domicile de l'électeur son identifiant et son mot de passe dans deux courriers postaux distincts ?

Non.

Conformément à la recommandation de la CNIL relative à la sécurité des systèmes de vote par correspondance électronique du 25 avril 2019, les solutions de vote dont le scrutin présente un risque de niveau 2 doivent atteindre à minima l'ensemble des objectifs de sécurité de niveau 1 et de niveau 2, dont l'objectif de sécurité n°2-04: « *Authentifier les électeurs en s'assurant que les risques majeurs et mineurs liés à une usurpation d'identité sont réduits de manière significative* ».

Si l'authentification des électeurs sur la plateforme de vote repose sur l'utilisation d'un couple identifiant/mot de passe, la CNIL recommande que ces derniers soient dédiés à l'élection et remis aux électeurs de manière sécurisée, via deux canaux de communication distincts définis avant l'élection, afin de réduire les risques d'interception par un tiers.

La CNIL recommande par ailleurs de compléter ce processus d'authentification en demandant à l'électeur de répondre à une question secrète non triviale dont il est le seul à connaître la réponse avec le responsable de traitement (sont par exemple exclus la date de naissance, le code postal, le numéro de département et tout autre élément facilement décelable).

Dans ce cadre, la voie postale constitue bien un seul et unique canal de communication, même si les envois de l'identifiant et du mot de passe se font par courriers distincts et à des dates différentes.

Cette solution n'est donc pas satisfaisante.

Pour la transmission de ces moyens d'authentification, la CNIL recommande de privilégier deux canaux parmi :

- la remise en mains propres sur le lieu de travail,
- l'envoi sur une adresse e-mail professionnelle ou un téléphone professionnel,
- l'envoi postal au domicile de l'électeur ,
- le dépôt sur un intranet professionnel ou un coffre-fort numérique accessibles au seul salarié.

Il convient dans tous les cas de s'assurer que les canaux choisis ne sont pas tous deux accessibles à un même tiers.

- Si le prestataire de solution de vote par correspondance électronique n'envisage pas de transmettre l'identifiant et le mot de passe par des canaux distincts, peut-il faire signer à l'organisateur du vote une décharge de responsabilité ?

Non.

L'identifiant et le mot de passe devraient être transmis par des canaux distincts : la signature d'une décharge de responsabilité est sans effet.

- Le mot de passe de l'électeur peut-il lui être envoyé en clair ?

Non, sauf par voie postale.

À l'exception des envois par voie postale, la CNIL recommande que les mots de passe permettant l'accès à la plateforme de vote en ligne ne soient jamais communiqués à l'utilisateur en clair, notamment par courrier électronique.

Il convient donc de privilégier, par exemple, l'envoi d'un lien à usage unique ou d'un mot de passe temporaire permettant à l'électeur de définir lui-même son mot de passe.

De plus, les mots de passe ainsi définis ne doivent pas faire l'objet d'un stockage en clair par le responsable de traitement ou un sous-traitant, conformément aux recommandations de la CNIL et de l'ANSSI.

- Les e-mails ou les numéros de téléphone personnels peuvent-ils être utilisés comme canaux de transmission des moyens d'authentification (identifiant et lien permettant la définition du mot de passe) ?

Non, sauf en cas de demande expresse de l'électeur (agent ou salarié) que l'employeur devra démontrer.

Pour les salariés du secteur privé, l'article L. 1121-1 du code du travail mentionne que « *nul ne peut apporter aux droits des personnes et aux libertés individuelles et collectives de restrictions qui ne seraient pas justifiées par la nature de la tâche à accomplir ni proportionnées au but recherché* ».

S'il est légitime que des données personnelles des salariés soit utilisées dans le cadre de l'organisation des élections de leurs représentants du personnel, l'utilisation de données issues du cadre privé à des fins professionnelles apparaîtrait disproportionnée dès lors qu'une autre solution est possible. Cela altérerait la frontière entre vie personnelle et vie professionnelle.

Des canaux de transmission autres que les numéros de téléphone et les adresses e-mails personnels des agents/salariés peuvent la plupart du temps être utilisés.

Par exemple, pour transmettre ses moyens d'authentification au salarié, il est possible de lui adresser un courrier postal à son domicile, de les lui envoyer par le biais de sa messagerie ou de son téléphone professionnels, de les lui remettre en mains propres sur son lieu de travail, ou de les rendre accessibles via un intranet professionnel ou un coffre-fort numérique accessibles au seul salarié.

- Les mêmes identifiants et mots de passe peuvent-ils être utilisés lors des deux tours d'une élection ?

Oui.

La CNIL considère que la connexion sur la plateforme de vote par correspondance électronique peut se faire à l'aide des mêmes identifiants lors des deux tours d'une élection.

- Quel secret complémentaire la CNIL conseille-t-elle d'utiliser pour sécuriser l'authentification des électeurs ?

Le secret complémentaire peut par exemple être défini selon les modalités suivantes :

- par le responsable de traitement ou l'électeur lui-même en amont de l'élection,
 - ou par la reprise d'une partie de l'IBAN (*International Bank Account Number*) de l'électeur,
 - ou par l'utilisation d'une donnée déjà transmise à l'électeur, par exemple les derniers chiffres du salaire d'une fiche de paie antérieure,
 - ou par le recours à un autre identifiant interne non public tel qu'un numéro de matricule affecté à l'agent à l'occasion de son service.
- Quelle procédure la CNIL conseille-t-elle d'utiliser pour la réinitialisation des moyens d'authentification, lorsque l'organisateur de l'élection ne souhaite pas collecter de données personnelles supplémentaires sur l'électeur ?

La seule vérification des nom, prénom, date et lieu de naissance de l'agent qui solliciterait la mise en œuvre de la procédure de réassort (réinitialisation des moyens d'authentification, par exemple en cas de perte ou d'oubli) n'est pas suffisante, ces informations pouvant aisément être connues de tiers (arrêt du Conseil d'État du 26 janvier 2021 n° 437989).

Dans la mesure où seuls l'électeur, l'organisateur de l'élection (le responsable de traitement) et, s'il en a un, son sous-traitant (le prestataire de vote) doivent être en possession de la réponse à la question secrète, il peut être envisagé de redemander cette réponse lors de la procédure de réinitialisation, en complément de la vérification des nom, prénom, date et lieu de naissance.

Une telle procédure permet de ne pas collecter davantage de données personnelles que celles déjà détenues par l'employeur.

- L'IBAN (International Bank Account Number) complet peut-il être utilisé par l'organisateur de l'élection ou son prestataire de solution de vote électronique comme question secrète ?

Non.

La CNIL estime que l'IBAN complet ne devrait pas être utilisé, et recommande de privilégier l'utilisation d'une partie de l'IBAN (par exemple les 5 derniers chiffres) en tant que secret complémentaire (question-défi) entre l'électeur et le responsable de traitement organisant le vote ou son prestataire de solution de vote électronique (sous-traitant).

L'utilisation d'un tel secret vient renforcer la sécurité de l'authentification par identifiant et mot de passe.

Pour que l'utilisation d'un morceau de l'IBAN soit légale, il est nécessaire de respecter l'une des deux conditions suivantes :

- la finalité « organisation des élections professionnelles » a été prévue dans le traitement qui a occasionné la collecte de l'IBAN,
 - sinon, l'organisateur de l'élection doit informer ses agents /salariés que l'IBAN va être utilisé pour cette finalité, si cela n'a pas été fait au moment de la collecte de la donnée.
- Quelles modalités doit respecter l'expertise de la solution de vote électronique ?

La CNIL considère que l'expertise doit couvrir l'intégralité du dispositif installé avant le scrutin (logiciel, serveur, etc.), la constitution des listes d'électeurs et leur enrôlement, ainsi que le fonctionnement du système de vote durant le scrutin et les étapes postérieures au vote (dépouillement, archivage, etc.).

L'expertise concerne ainsi plusieurs aspects du dispositif de vote :

- le logiciel de vote en lui-même,
- l'organisation du scrutin (constitution des listes électorales, envoi des identifiants de connexion aux électeurs, information, etc.),
- le déploiement du système de vote,
- le scrutin en lui-même.

Dans le cas où l'organisateur de l'élection met en place un système de vote pour plusieurs entités, une seule et même expertise peut être réalisée pour garantir la conformité du logiciel de vote, du mode d'organisation du scrutin et du déploiement du système de vote (étapes 1, 2 et 3 ci-dessus), à la condition que ces derniers soient parfaitement identiques pour toutes les entités et que l'entité puisse le prouver techniquement.

En revanche, l'expertise doit normalement veiller au bon déroulement de chacun des scrutins de manière individuelle, notamment pour le scellement et le dépouillement des urnes (étape 4 ci-dessus) : cette partie de l'expertise ne peut donc pas être réutilisée à priori.

Il s'agit du cas, par exemple, d'un centre de gestion qui assure l'organisation des élections pour toutes les collectivités territoriales qui lui sont affiliées.

À l'exception de la fonction publique de l'État, cette expertise n'est pas à transmettre à la CNIL, sauf demande de sa part.