

Politique de protection des données : dispositif d'alerte éthique

1. Informations sur la mise en œuvre d'un traitement de données à caractère personnel

La Direction de l'Éthique Groupe au sein de la Société Nationale SNCF (DEG) met en œuvre dans le cadre du dispositif de recueil des alertes éthiques un traitement automatisé de données à caractère personnel, conformément aux article 8.I.B et 17.II.2° de la loi Sapin II et l'article L.225-102-4 du code de commerce issu de la loi n°2017-399 du 27 mars 2017 relative au devoir de vigilance des sociétés mères et des entreprises donneuses d'ordre.

2. Finalité et base légale du traitement

Ce traitement est mis en œuvre afin de recueillir et traiter les alertes déposées sur la plateforme d'alerte en ligne alrteethiquesncf.com, reçues par la DEG par un autre canal écrit (mail, courrier postal) ou allouées à la DEG.

Plus précisément, la DEG collecte des données dans le cadre du présent traitement afin de :

- recueillir et analyser la recevabilité des signalements visant à révéler un :
 - o un crime, un délit ;
 - o une atteinte grave aux droits humains et libertés fondamentales, à la santé et à la sécurité des personnes ou à l'environnement ;
 - o une menace ou un préjudice pour l'intérêt général, ou
 - o une violation ou une tentative de dissimulation d'une violation :
 - d'un engagement international régulièrement ratifié ou approuvé par la France;
 - d'un acte unilatéral d'une organisation internationale pris sur le fondement d'un tel engagement ;
 - du droit de l'union européenne ;
 - de la loi ou du règlement, ou
 - de la charte éthique Groupe, du code de conduite ou de politiques déclinées en application de ces référentiels d'entreprise.
- attribuer les alertes éthiques au référent alerte de l'entité compétente la plus proche des faits au sein du groupe public unifié (Société Nationale SNCF, SNCF Voyageurs, SNCF Réseau, SNCF Gares & Connexions, FRET SNCF et R4L (périmètre RLE), leurs filiales ou entités contrôlées hors KEOLIS et GEODIS) ;
- traiter les alertes pour lesquelles un risque de conflits d'intérêts ou un enjeu d'impartialité est identifié ;

- traiter les alertes critiques ou complexes ainsi que celles dont les allégations mettent en cause, par exemple, la réputation de la SNCF ou les instances dirigeantes de SA/SAS ou d'entités contrôlées ;
- gérer, améliorer et contrôler le dispositif d'alerte éthique (statistiques, accompagnement du réseau des référents alerte et contrôle).

Le traitement repose sur :

- l'obligation légale d'établir une procédure interne de recueil et de traitement des signalements prescrite par l'article 8.I.B de la loi Sapin II, l'article 17.II.2° de la loi Sapin II et l'article L.225-102-4 du code de commerce issu de la loi relative au devoir de vigilance des sociétés mères et des entreprises donneuses d'ordre ;
- l'intérêt légitime de la DEG de recueillir tout signalement révélant une violation ou tentative de dissimulation d'une violation de la charte éthique Groupe ou de politiques déclinées en application des référentiels d'entreprise ;
- le consentement du lanceur d'alerte à l'attribution de l'alerte ;
- l'intérêt légitime de la DEG concernant la gestion, l'amélioration et le contrôle du dispositif d'alerte éthique (statistiques, accompagnement du réseau des référents alertes et contrôle).

3.Catégories de données traitées

Les catégories de données traitées sont :

- identité, fonctions et coordonnées de l'émetteur de l'alerte ;
- identité, fonctions et coordonnées des personnes faisant l'objet de l'alerte ;
- identité, fonctions et coordonnées des personnes intervenant dans le recueil ou dans le traitement de l'alerte ;
- faits signalés ;
- éléments recueillis dans le cadre de la vérification des faits signalés ;
- compte rendu des opérations de vérification ;
- suites données à l'alerte.

4.Destinataires des données

Conformément à l'article 6 du décret n°2022-1284 du 3 octobre 2022, la DEG garantit l'intégrité et la confidentialité des informations recueillies dans un signalement déposé sur la plateforme.

4.1.Les destinataires externes

Afin d'assurer la bonne gestion de la plateforme d'alerte en ligne accessible à l'adresse alerteethiquesncf.com, la DEG sous-traite les données à caractère personnel collectées dans le cadre du dispositif d'alerte éthique à la société Business Keeper GmbH, prestataire ayant son siège social au sein de l'Union européenne et hébergeur de la plateforme de recueil des alertes sur des serveurs basés au sein de l'Union européenne.

Pour les besoins du traitement d'une alerte, les données collectées par la DEG peuvent être communiquées à un professionnel externe (ex : traducteur, expert, cabinet d'avocat, consultants, etc.).

Les données collectées peuvent être transmises à l'autorité judiciaire dans le cas d'une procédure judiciaire ou en cas de réquisition des rapports d'enquête interne par l'autorité judiciaire (dans ce cas le référent alerte en informe le lanceur d'alerte sauf si cela risque de compromettre la procédure judiciaire¹).

4.2. Les destinataires internes

Sauf en cas de conflit d'intérêts, d'enjeu d'impartialité, lorsque l'alerte est de nature critique ou complexe ou lorsque l'alerte concerne des allégations mettant en cause, par exemple, la réputation de la SNCF ou les instances dirigeantes de SA/SAS ou d'entités contrôlées, les alertes sont transférées, avec l'accord du lanceur d'alerte, au référent alerte de l'entité compétente la plus proche des faits, au sein du groupe SNCF :

- Société Nationale SNCF,
- SNCF Voyageurs,
- SNCF Réseau,
- SNCF Gares & Connexions
- FRET SNCF et R4L (périmètre RLE),
- Leurs filiales ou entités contrôlées hors KEOLIS et GEODIS,

Les données à caractère personnel collectées par la DEG peuvent dans le cadre d'une enquête interne être communiquées :

- au président de la Société Nationale SNCF ;
- au représentant légal de l'entité concernée
- au directeur des ressources humaines du Groupe Public Unifié ;
- au DGD stratégie finances ;
- à la direction de la sûreté lorsque les dysfonctionnements révélés par le signalement justifient leur concours, sur instructions de la DEG ;
- à tout responsable en mesure de mettre en œuvre les recommandations ou de donner toutes instructions utiles à cette fin.

5. Droits des personnes concernées

Toute personne concernée par un traitement de données à caractère personnel dispose, dans les conditions et limites prévues par la réglementation, du droit de demander l'accès à ses données à caractère personnel, la rectification ou l'effacement de celles-ci, la limitation du traitement la concernant, ou, le cas échéant, de s'opposer à au traitement/retirer son consentement. La personne souhaitant exercer tout ou partie de ces droits est invitée, sur

¹ Loi Sapin II n° 2016-1691 du 9-12-2016 art. 9.I.

justification de son identité par tout moyen vérifiable, à adresser sa demande à l'adresse e-mail ligneethique@sncf.fr.

Une réponse sera adressée dans un délai d'un mois suivant la réception de la demande. Au besoin, ce délai pourra être prolongé de deux mois supplémentaires. Dans ce cas, la personne en sera informée, avec les motifs de la prolongation.

Il ne pourra être fait droit à une demande de droit d'accès qui serait susceptible de porter atteinte aux droits et libertés des tiers. L'exercice de ce droit ne doit pas permettre à la personne qui l'exerce d'accéder aux données à caractère personnel d'autres personnes physiques. Ainsi, la DEG peut refuser toute demande d'accès qui porterait atteinte au droit des témoins entendus à garder l'anonymat, à la confidentialité de l'identité du lanceur d'alerte ainsi qu'au droit du lanceur d'alerte d'être garanti de toute mesure de représailles.

L'exercice du droit à la rectification des données ne doit pas permettre la modification rétroactive des éléments contenus dans l'alerte ou collectées lors de son instruction. Son exercice, lorsqu'il est admis, ne doit pas aboutir à l'impossibilité de reconstitution de la chronologie des éventuelles modifications d'éléments importants de l'enquête. Ainsi, ce droit ne peut être exercé que pour rectifier les données factuelles, dont l'exactitude matérielle peut être vérifiée par la DEG à l'appui d'éléments probants, et ce sans que soient effacées ou remplacées les données, même erronées, collectées initialement.

Le droit d'opposition ne peut être exercé à l'égard des traitements, dont la finalité repose sur l'obligation légale de mettre en œuvre un dispositif de recueil et de traitement des données (v. les articles 8.I.B et 17.II.2° de la loi Sapin II et l'article L.225-102-4 du code de commerce issu de la loi n°2017-399 du 27 mars 2017).

Pour information, la SNCF a désigné un délégué à la protection des données dont les coordonnées sont : dpo-sncf@sncf.fr.

Si une personne devait considérer que le traitement qui la concerne constitue une violation de la réglementation, elle dispose du droit d'introduire une réclamation auprès de la Commission nationale de l'informatique et des libertés (CNIL Service des plaintes 3 place de Fontenoy TSA 80715 75334 Paris cedex 17) ou de l'autorité de contrôle de l'Etat où se trouve sa résidence habituelle, son lieu de travail, ou le lieu où la violation prétendue aurait été commise.

6. Durées de conservation des données

Conformément à l'article 9.III de la loi Sapin II et aux recommandations de la Cnil, les données à caractère personnel collectées par la DEG lors du traitement d'une alerte sont conservées pendant la durée nécessaire à la réalisation des finalités du traitement exposées au point 2.2 ci-dessus et à la protection de leurs auteurs, des personnes visées et des tiers

mentionnés dans ces signalements, en tenant compte des délais d'éventuelles enquêtes complémentaires :

- les données relatives à une alerte n'entrant pas dans le champ d'application du dispositif d'alertes sont conservées en archivage intermédiaire pendant 6 mois maximum à compter de la clôture du signalement, puis détruites.
- les données relatives à une alerte entrant dans le champ d'application du dispositif sont conservées en base active, jusqu'à la prise de la décision définitive sur les suites données à l'alerte (y compris la mise en œuvre effective du plan d'action associé au rapport d'enquête) puis 6 ans en archivage intermédiaire.
- lorsqu'une procédure disciplinaire est engagée à l'encontre d'une personne mise en cause ou de l'auteur d'une alerte abusive, les données relatives à l'alerte sont conservées 3 ans en base active à compter de la date de la fin du processus disciplinaire puis 3 ans en archive intermédiaire.
- lorsqu'une procédure contentieuse est engagée à l'encontre d'une personne mise en cause ou de l'auteur d'une alerte abusive, les données sont conservées jusqu'à l'extinction des voies de recours ordinaires et extraordinaires contre la décision rendue ;
- lorsqu'une juridiction judiciaire, administrative, arbitrale, ou que l'inspection du travail ou une autorité externe figurant en annexe du décret n°2022-1284 du 3 octobre 2022 est saisie, impliquant ou mettant en cause une des sociétés du groupe SNCF, les données sont conservées jusqu'à l'extinction des voies de recours ordinaires et extraordinaires contre la décision rendue.

7. Les flux transfrontières

La DEG est susceptible de transférer des données personnelles en dehors de l'Union européenne dans le cadre du recueil et du traitement des alertes.

Lorsque c'est le cas, le transfert peut avoir lieu sur la base d'une décision rendue par la Commission européenne, lorsque celle-ci a reconnu que le pays dans lequel les données sont transférées assure un niveau de protection adéquat. À défaut de décision d'adéquation, la DEG prendra toutes les mesures nécessaires pour assurer la protection des données à caractère personnel transférées sur la base de garanties appropriées (clauses contractuelles types approuvées par la Commission européenne ou autres outils de transfert visés au chapitre V du RGPD, complétés par des mesures adéquates, le cas échéant).

Dans tous les cas, la DEG prend des mesures pour sécuriser les flux de données transfrontières notamment :

- par l'utilisation du système sécurisé BKMS pour le recueil des alertes éthiques dont les serveurs sont localisés au sein de l'Union européenne ;
- par la mise en œuvre de mesures organisationnelles en interne afin de protéger les données.