ENEDIS
L'ELECTRICITE EN RESEAU

CONFORMITÉ DES AFFAIRES
Dispositif d'alertes

Guide du lanceur d'alerte

Juin 2019

Introduction

La loi Sapin 2 du 9 décembre 2016, relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique, crée un statut unique du « lanceur d'alerte ». Elle le définit, organise la procédure de signalement, et lui consacre un régime commun de protection.

Afin de répondre aux exigences de cette loi, Enedis fait évoluer son dispositif d'alertes existant. Il permet de signaler un manquement au code anticorruption, une atteinte grave envers les droits humains et les libertés fondamentales, la santé-sécurité des personnes ou l'environnement. **Il s'agit d'un dispositif complémentaire aux autres canaux de signalement qui existent dans l'entreprise. Son utilisation ne constitue aucune obligation pour le salarié. Ce dispositif est également mis à disposition des tiers.**

L'objectif de ce guide est notamment de préciser :
- les personnes pouvant émettre un signalement ;
- les faits pouvant faire l'objet d'un signalement ;
- la procédure à suivre pour émettre un signalement ;
- les modalités de recevabilité et de traitement d'un signalement ;

et de présenter :
- le régime de protection du lanceur d'alerte prévu par la loi Sapin 2 ;
- les modalités de protection, d'accès et de rectification des données à caractère personnel.

Le respect de la politique Conformité des Affaires Enedis est une volonté affirmée de l'instance dirigeante. Au sein d'Enedis, le référent du dispositif d'alertes est la Déléguée Éthique, Sécurité du Patrimoine et Conformité des Affaires.

Si cette politique est rigoureuse et qu'elle doit être scrupuleusement suivie, c'est d'une part, parce que telle est la loi, et d'autre part, parce qu'y contrevenir peut avoir des conséquences désastreuses pour l'entreprise et ses partenaires.

Voilà pourquoi il est de la responsabilité de chacun d'entre nous de bien en comprendre l'esprit et de s'y conformer. Être irréprochable consolide durablement la confiance placée dans l'entreprise.

1. Les principes généraux du dispositif d'alertes Enedis

Avertir d'une infraction, d'un manquement aux obligations d'Enedis, ou prévenir d'un danger, c'est intervenir dans l'intérêt général, préserver la sécurité des salariés ainsi que leur intégrité physique et morale, et protéger l'entreprise.
En effet, si l'entreprise ignore qu'un manquement a été commis, elle ne peut pas prendre les mesures nécessaires pour y mettre fin.

Pour bénéficier du régime protecteur lié au statut de lanceur d'alerte, vous êtes tenu de respecter les trois conditions cumulatives suivantes :

- **répondre à la définition du lanceur d'alerte (cf. § 1.1) ;**
- **révéler des faits entrant dans le champ de la loi (cf. § 1.2) ;**
- **respecter impérativement la procédure définie au § 1.3.**

1.1. Qui peut être lanceur d'alerte ?

Pour être lanceur d'alerte, vous devez remplir les conditions ci-dessous :

- être une personne physique (les personnes morales étant exclues du dispositif) ;
- avoir eu personnellement connaissance des faits vous paraissant devoir être signalés ;
- signaler de manière désintéressée, c'est-à-dire sans espérer une contrepartie ou tirer un avantage, notamment financier du signalement ;
- être de bonne foi, c'est-à-dire sans chercher à nuire à autrui ;
- avoir des raisons légitimes de croire à la véracité des faits signalés.

1.2. Quels faits peuvent faire l'objet d'un signalement ?

Les faits signalés doivent relever de l'une des catégories suivantes :

- Tout manquement aux valeurs et principes d'action d'Enedis ;
- le non-respect du code anticorruption ;
- une atteinte grave aux droits humains et aux libertés fondamentales ;
- une atteinte grave à la santé et à la sécurité des personnes ;
- une atteinte grave à l'environnement qui résulterait des activités ;
- un crime ou un délit ;
- une violation grave et manifeste :
  – d'une disposition légale ou réglementaire ;
  – d'un engagement international ratifié ou approuvé par la France ;
  – d'un acte unilatéral d'une organisation internationale, pris sur le fondement d'un engagement international ratifié ou approuvé par la France ;
- une menace ou un préjudice grave pour l'intérêt général.

Les faits, informations ou documents, quels que soient leur forme ou leurs supports, couverts par le secret de la défense nationale, le secret médical ou le secret de la relation entre un avocat et son client, ne peuvent pas faire l'objet d'un signalement.

Les autres secrets protégés par la loi (secret de fabrication ou de procédé, secret bancaire, etc.) peuvent être signalés si leur divulgation est *« nécessaire et proportionnée à la sauvegarde des intérêts en cause »*, et respecte la procédure de signalement prévue au § 1.3.

1.3. Quelle procédure suivre pour émettre un signalement ?

La procédure de signalement concerne les salariés d'Enedis, ainsi que les collaborateurs extérieurs et / ou occasionnels. Elle doit être graduelle et respecter l'ordre suivant :

- ***signalement interne :*** vous devez en premier lieu signaler les faits en interne, auprès de votre manager direct ou indirect, employeur ou référent désigné par l'entreprise, ou par le biais du dispositif d'alertes mis à votre disposition (cf. § 2) ;
- ***signalement externe :*** si la vérification interne de la recevabilité du signalement ne se fait pas dans un délai raisonnable, vous pouvez vous adresser à l'autorité judiciaire, à l'autorité administrative ou aux ordres professionnels compétents ;
- ***signalement public :*** en dernier ressort, à défaut de traitement par lesdites autorités dans un délai de trois mois après leur saisine, vous pouvez rendre le signalement public.

Vous pouvez saisir, à tout moment, le Défenseur des Droits au sujet d'une alerte que vous souhaiteriez soumettre, afin d'être orienté vers l'organisme compétent à la recevoir.

1.4. *Quid* des signalements émis en dehors du dispositif d'alertes ?

Le recours au dispositif d'alertes n'est pas obligatoire. D'autres canaux de signalement existent au sein de l'entreprise.
Les faits peuvent être portés directement à la connaissance du management, des acteurs médico-sociaux, des partenaires sociaux, du Référent Contrôle Interne (RCI) d'entité, ou de manière orale, par courrier postal ou courriel à la Déléguée Éthique (delegation-ethique@enedis.fr).
En cas de signalement *via* un autre canal que celui du dispositif d'alertes Enedis, décrit au § 2, et afin de bénéficier de l'intégralité des avantages de ce dispositif, notamment en termes de confidentialité et de la protection que lui accorde la loi Sapin 2, le lanceur d'alerte sera invité par son interlocuteur à enregistrer également le signalement dans le dispositif d'alertes.

Le signalement pourra, le cas échéant, être enregistré dans le dispositif à des fins statistiques et sans mention de l'identité du lanceur d'alerte ou des personnes mises en cause.

2. Le recueil des signalements

2.1. Une adresse Internet dédiée

La personne qui souhaite signaler des faits *via* le dispositif d'alertes, doit remplir un formulaire de signalement disponible sur un site externe à l'entreprise à l'adresse suivante : https://www.bkms-system.com/alertes-enedis.
Il est aussi accessible *via* les sites Internet et intranet Enedis. Il s'agit d'une **adresse Internet dédiée et sécurisée,** qui permet au lanceur d'alerte de disposer d'un canal de signalement simple et accessible 24 heures sur 24 et 7 jours sur 7, où qu'il soit et à partir d'une variété de supports (ordinateurs, tablettes et smartphones).

2.2. Le formulaire de signalement et les catégories de données enregistrées

Ce formulaire comprend des champs à remplir afin que le signalement puisse être étudié. Un tutoriel d'utilisation du dispositif d'alertes est mis à disposition sur les sites internet et intranet Enedis.
Conformément au Règlement Européen sur la Protection des Données (RGPD) et aux dispositions d'Enedis relatives au traitement des données à caractère personnel, les principales catégories de donnés enregistrées sont les suivantes :

- **le domaine concerné par le signalement :** corruption, atteinte à l'environnement, harcèlement, etc. ;
- **votre identité (sauf à ce que vous souhaitiez conserver l'anonymat) :** votre nom, vos coordonnées, votre fonction ;
- **l'objet du signalement et son descriptif ;**
- **votre relation avec Enedis :** salarié, collaborateur externe ou occasionnel, tiers externe à l'entreprise.

Vous pouvez également joindre des pièces pour justifier les faits signalés et les noms des témoins éventuels. Vous devez présenter des faits entrant dans le champ de la loi (cf. § 1.2).
La saisie de tous les champs n'est pas obligatoire.

Pour autant, si les informations fournies sont insuffisantes pour vérifier les faits signalés, la Délégation Éthique - Sécurité du Patrimoine et Conformité des Affaires (DESP et Conformité des Affaires), qui est en charge de l'analyse de la recevabilité de votre signalement, reviendra vers vous pour obtenir des informations complémentaires.

Vous êtes également invité à choisir le domaine duquel relève votre alerte. Le Référent Enedis recevra votre alerte et la transmettra au responsable de traitement associé au domaine que vous avez choisi (cf. § 3.3), sauf s'il estimait que cette alerte relève d'un autre domaine. Dans ce dernier cas, le Référent Enedis pourra transmettre l'alerte au responsable de traitement concerné. Quel que soit le responsable de traitement, la DESP et Conformité des Affaires assurera un suivi de l'avancement du traitement.

À l'issue de l'étape de signalement, un identifiant personnel et un mot de passe vous seront fournis, afin que vous puissiez suivre l'évolution du traitement de votre signalement.

Si besoin, cet identifiant vous permettra également de dialoguer avec le responsable du traitement.

2.3. Le respect de la confidentialité

Si vous le souhaitez, vous pouvez vous identifier lorsque vous signalez des faits via le dispositif d'alertes. Votre identité est traitée **de façon confidentielle** par les personnes chargées de l'examen de la recevabilité et du traitement de votre signalement. Enedis a pris les mesures appropriées pour garantir le respect de la confidentialité de votre identité, de celle des personnes citées, ainsi que des faits signalés.

Le respect de la confidentialité est notamment assuré par les dispositions suivantes :

- conformément à l'article 9 de la loi Sapin 2, les éléments de nature à vous identifier ne peuvent être divulgués, sauf à l'autorité judiciaire et seulement avec votre consentement. Si, pour les besoins du traitement du signalement, il s'avérait nécessaire de communiquer votre identité, votre accord vous serait demandé préalablement ;

- au nom du respect de la présomption d'innocence, les éléments de nature à identifier les personnes mises en cause par un signalement ne peuvent être divulgués, sauf à l'autorité judiciaire, et une fois le caractère fondé du signalement établi ;
- le formulaire de signalement est accessible sur un site Web extérieur à l'entreprise, qui ne conserve pas les métadonnées (effacement des adresses IP lors de la connexion) ;
- un engagement de confidentialité est individuellement signé par la DESP et Conformité des Affaires en charge de l'analyse de la recevabilité des signalements, ainsi que par toute personne impliquée dans leur traitement (manager, RCI, expert métier, etc.), préalablement à leur accès aux données extraites du dispositif d'alertes ;
- toutes les données saisies et les rapports résultant des vérifications enregistrés dans le dispositif sont cryptés ;
- seul le Référent Enedis dispose des clés de déchiffrement. Ce dernier habilite les responsables de traitement du signalement à consulter les données ;
- tous les échanges entre un lanceur d'alerte et le responsable du traitement sont réalisés à l'intérieur du système sécurisé et crypté, sans recours à une messagerie externe au dispositif ;
- afin d'assurer la traçabilité des personnes accédant aux données, chaque cas traité dispose d'un journal de processus qui trace l'intégralité des actions effectuées par les différentes personnes ayant accès au signalement.

Si vous souhaitez rester anonyme, vous pourrez continuer à dialoguer avec les personnes en charge de l'examen de votre signalement, grâce à l'identifiant personnel et au mot de passe qui vous auront été fournis à l'issue de l'enregistrement dans le dispositif.
Si le signalement est anonyme, les conditions de recevabilité feront l'objet d'un examen renforcé (reconnaissance de la gravité des faits, niveau de précision des éléments factuels, etc.).

2.4. La protection des lanceurs d'alerte

Dès lors que vous remplissez les conditions pour bénéficier du statut de lanceur d'alerte (cf. § 1), vous bénéficiez de la protection qui vous est accordée par la loi.

Vous bénéficiez de la protection professionnelle : aucune sanction ou mesure discriminatoire directe ou indirecte ne peut être prise à votre égard dans le respect des exigences de la loi :

- vous ne pouvez pas être sanctionné ou licencié du fait de votre signalement ;
- vous ne pouvez pas faire l'objet d'une mesure discriminatoire du fait de votre signalement, notamment en matière de rémunération, de mesures d'intéressement, de formation, de reclassement, d'affectation, de qualification, de classification, de promotion professionnelle, de mutation ou de renouvellement de contrat.

Dans certaines conditions, vous bénéficiez d'une immunité pénale en cas de violation d'un secret légalement protégé, autre que ceux couverts par le secret de la défense nationale, le secret médical ou le secret des affaires.

2.5. Les risques encourus par un lanceur d'alerte dénonçant des faits de mauvaise foi

Effectuer un signalement de mauvaise foi, dans l'intention de nuire ou en ayant connaissance du caractère mensonger des faits signalés, peut être lourd de conséquences pour le lanceur d'alerte, même si les faits sont finalement avérés :

- vous ne bénéficiez plus de la protection de la loi ;
- vous encourez alors des sanctions disciplinaires ;
- vous êtes susceptible d'être poursuivi pénalement (potentiellement pour diffamation) ;
- vous engagez également votre responsabilité civile et risquez d'être condamné à réparer le préjudice subi par la victime de votre signalement mensonger.

En revanche, aucune mesure ne sera engagée contre vous si vous utilisez le dispositif de bonne foi, quand bien même les faits ne s'avéreraient pas fondés après leur vérification.

3. Le traitement des signalements

3.1. La réception des signalements

Les personnes habilitées à recevoir les signalements au sein de la Délégation Éthique - Sécurité du Patrimoine et Conformité des Affaires sont en nombre très limité.

Dès que le signalement est validé par le lanceur d'alerte dans le dispositif, le Référent Enedis en est averti. Celui-ci examine les données fournies et vous adresse un accusé de réception dans les 72 heures, qui mentionnera le délai raisonnable nécessaire pour en vérifier la recevabilité.

3.2. La recevabilité du signalement

Chaque signalement fait l'objet d'un examen de recevabilité — sous un délai raisonnable qui ne pourra excéder un mois — par la DESP et Conformité des Affaires, afin de déterminer, avant le lancement des vérifications, s'il entre dans le champ d'application du dispositif d'alertes Enedis.

- Si le signalement est recevable, son analyse est confiée selon sa nature (corruption, éthique, devoir de vigilance, etc.), par le Référent Enedis, au responsable de traitement compétent ;
- Si le signalement n'est pas recevable, les données saisies sont immédiatement supprimées, et vous en serez informé. Deux possibilités peuvent alors se présenter :
  – Vous pouvez être averti de la non recevabilité de votre signalement ainsi que de son motif ;
  – Vous pouvez être réorienté vers d'autres interlocuteurs.
- Si besoin, la DESP et Conformité des Affaires échangera avec vous de manière sécurisée, afin d'obtenir les informations nécessaires à la finalisation de l'analyse de recevabilité de votre alerte.

3.3. La vérification des faits signalés

Après analyse de la recevabilité du signalement, celui-ci fait l'objet d'un traitement dans les trois mois. Si nécessaire, le délai peut être prolongé avec votre accord afin de finaliser l'instruction.

Le responsable du traitement de votre signalement est alors nommément identifié et dûment habilité par la DESP et Conformité des Affaires (délivrance des droits d'accès, signature de l'engagement de confidentialité, etc.). Celui-ci disposera des délégations de pouvoir et de la formation nécessaires pour procéder aux vérifications de la réalité des faits signalés.

Les faits signalés peuvent être vérifiés avec l'appui éventuel d'experts métiers, des Référents Contrôle Interne (RCI) d'entité, de directions support (Direction Ressources Humaines, Transformation Santé Sécurité - DRHTS, Direction des Systèmes d'Information – DSI, Direction des Affaires Juridiques – DRAJ, Direction Audit et Contrôle Interne – DACIR, etc.) ou encore, lorsque cela s'avère nécessaire, d'un conseil externe, soumis aux mêmes règles de confidentialité.

Dans le cas où la vérification de la réalité des faits signalés nécessite la communication de votre identité, une demande formelle de levée de confidentialité vous sera adressée préalablement. Si vous ne souhaitez pas lever cette confidentialité et que, consécutivement à ce refus, l'examen des faits ne peut être poursuivi, vous serez informé de l'arrêt du traitement.

À l'issue de la vérification des faits :

- si les faits signalés sont avérés, le responsable du traitement émet ses recommandations pour faire cesser le dysfonctionnement à l'origine de votre signalement. Celles-ci sont adressées au management de la personne visée par le signalement. Les actions correctives estimées nécessaires ainsi que les sanctions éventuelles sont engagées, et la DESP et Conformité des Affaires en est informée ;
- si les faits signalés ne sont pas avérés, le responsable du traitement clôt le dossier et en informe la DESP et Conformité des Affaires.

3.4. L'information du lanceur d'alerte

Si votre signalement est recevable, le nom de la personne désignée responsable de son traitement vous sera communiqué par la DESP et Conformité des Affaires.

Vous pourrez suivre l'état d'avancement du traitement de votre signalement en vous connectant au dispositif d'alertes Enedis avec vos identifiant et mot de passe.

Vous serez également averti si le délai de traitement doit être prorogé au-delà des trois mois prévus initialement.

À l'issue de la vérification des faits signalés, et quelle qu'en soit l'issue, vous serez informé du résultat du traitement ainsi que de la clôture du dossier.

3.5. L'information des personnes visées par le signalement

Si le signalement est recevable, la personne mise en cause est informée des faits qui lui sont reprochés, afin de pouvoir faire usage de ses droits.

Il est rappelé que toute personne ayant fait l'objet d'un signalement est présumée innocente jusqu'à ce que les faits qui lui sont reprochés soient établis.

L'information de la personne mise en cause a lieu après que la recevabilité du signalement a été validée. Aucune information de la personne mise en cause n'est réalisée en cas de non-recevabilité du signalement puisque, dans ce cas, les données sont immédiatement effacées.

Si la personne potentiellement mise en cause doit en être informée, elle le sera de façon sécurisée par le responsable de traitement.

La personne en charge du traitement du signalement peut, si elle dispose d'éléments fiables et matériellement vérifiables, décider de prendre des mesures conservatoires, notamment pour prévenir la destruction des preuves ; cela en amont de l'information de la personne visée par le signalement.

3.6. Le reporting

Afin d'évaluer l'efficacité du dispositif d'alertes Enedis, la DESP et Conformité des Affaires met en place un suivi annuel statistique anonyme relatif à la réception, le traitement et les suites données aux signalements. Ce suivi permettra notamment de détecter les éventuels problèmes d'ordre éthique et de conformité nécessitant la mise en place d'actions préventives ou correctives.

Il consolidera le nombre de signalements reçus, de dossiers clos, de dossiers ayant donné lieu à un traitement, ainsi que le nombre et la nature des mesures prises pendant et à l'issue des vérifications des faits signalés (mesures conservatoires, procédure disciplinaire ou judiciaire, sanctions prononcées, etc.).

4. La gestion des données à caractère personnel

4.1. La protection des données à caractère personnel

En conformité avec les exigences de l'autorisation unique AU004 du 8 décembre 2005 modifiée, publiée par la Cnil, Enedis a mis en place un dispositif d'alertes impliquant un traitement automatisé des données à caractère personnel.

Ce dispositif répond aux exigences du Règlement Européen sur la Protection des Données (RGPD).

4.2. Le droit d'accès et de rectification

Conformément aux articles 39 et 40 de la loi Informatique et libertés du 6 janvier 1978, le lanceur d'alerte et la personne faisant l'objet d'un signalement peuvent accéder aux données les concernant et en demander, si elles sont inexactes, incomplètes, équivoques ou périmées, la rectification ou la suppression.

Les demandes sont à formuler auprès de DESP et Conformité des Affaires :

- soit par courrier à l'adresse suivante : Enedis – Tour Enedis – Déléguée Éthique et Sécurité du Patrimoine – Bureau 19-12 – 34, place des Corolles — 92079 La Défense Cedex ;
- soit par e-mail à l'adresse suivante : delegation-ethique@enedis.fr

Sur le fondement du droit d'accès, la personne mise en cause ne peut en aucun cas obtenir des informations concernant l'identité du lanceur d'alerte.

4.3. La conservation et l'archivage des données

Les données à caractère personnel relatives à un signalement considéré comme non recevable sont détruites sans délai.

Lorsque le signalement n'est pas suivi d'une procédure disciplinaire ou judiciaire, les données à caractère personnel sont détruites dans un délai de deux mois à compter de la clôture des opérations de vérification. Les autres éléments du dossier sont archivés à des fins statistiques ou de reporting après anonymisation.

Lorsqu'une procédure disciplinaire ou des poursuites judiciaires sont engagées à la suite d'un signalement, les données à caractère personnel sont conservées jusqu'au terme de la procédure.

Les données faisant l'objet de mesures d'archivage sont conservées de manière anonyme sur une plateforme sécurisée, pour une durée n'excédant pas les délais de procédures contentieuses.

5. L'information des utilisateurs potentiels du dispositif d'alertes Enedis

Le nouveau dispositif d'alertes Enedis, qui s'inscrit en complément des dispositifs existants, ainsi que ce guide seront portés à la connaissance de l'ensemble des salariés et collaborateurs externes ou occasionnels. Ils ont également fait l'objet d'une information auprès des instances représentatives du personnel.

Contacts

Pour tout complément d'information, nous vous invitons à contacter :

delegation-ethique@enedis.fr

Enedis – Secrétariat général – Délégation Éthique – Sécurité du Patrimoine et Conformité des Affaires
Tour Enedis – 34, place des Corolles – 92079 Paris La Défense Cedex – **enedis.fr**
SA à directoire et à conseil de surveillance au capital de 270 037 000 euros – RCS Nanterre 444 608 442

DOC 742 - Réalisation : éditss - www.edites.fr - Crédit photo : Istock – Juin 2019