RÉFÉRENTIEL

RELATIF AUX TRAITEMENTS DE DONNEE A CARACTERE PERSONNEL DESTINES A LA MISE EN ŒUVRE D'UN DISPOSITIF D'ALERTE

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

1. A qui s'adresse ce référentiel ?

Ce référentiel, pris en application des dispositions de l'article 11-I-a bis de la loi du 6 janvier 1978 modifiée, encadre la mise en œuvre des traitements de données à caractère personnel dans le cadre d'un dispositif d'alerte.

Il s'adresse aux organismes privés ou publics ainsi qu'aux services qui décideraient ou seraient tenus de mettre en œuvre un dispositif leur permettant de recueillir et traiter des signalements de conduites ou de situations susceptibles de constituer un manquement aux règles applicables dans leur entité.

Il peut s'agir, par exemple, d'un dispositif mis en œuvre par les organismes publics ou privés conformément à la loi dite « loi Sapin 2 »[1], d'un dispositif mis en œuvre en application de la « loi relative au devoir de vigilance »[2] ou encore d'un dispositif mis en œuvre par le comité social et économique pour recevoir les alertes de salariés[3].

2. Portée du référentiel

Les traitements visant à permettre le recueil et le traitement d'alertes, qu'ils soient mis en œuvre à partir d'outils internes ou externalisés auprès d'un prestataire de service, conduisent à collecter des données relatives à des personnes physiques identifiées ou identifiables (employés, salariés, stagiaires, etc.). A ce titre, ils sont soumis aux dispositions du Règlement général sur la protection des données (RGPD), de la loi du 6 janvier 1978 modifiée (LIL) ainsi qu'aux dispositions spécifiques relatives aux relations de travail (code du travail).

Les organismes concernés, en tant que responsables de traitement, doivent mettre en œuvre toutes les mesures techniques et organisationnelles appropriées afin de garantir un haut niveau de protection des données personnelles dès la conception des traitements et tout au long de la vie de ceux-ci. Ils doivent, en outre, être en mesure de démontrer cette conformité à tout instant. Les traitements mis en œuvre doivent être inscrits dans le registre prévu à l'article 30 du RGPD (voir les modèles de registre sur le site cnil.fr).

L'application de ce référentiel permet d'assurer la conformité des traitements de données mis en œuvre dans le cadre des dispositifs d'alerte aux principes relatifs à la protection des données.

Les organismes qui s'écarteraient du référentiel au regard des conditions particulières tenant à leur situation doivent être en mesure de justifier l'existence d'un tel besoin, puis prendre toutes les mesures appropriées à même de garantir la conformité des traitements à la réglementation en matière de protection des données à caractère personnel.

Ce référentiel constitue également une aide à la réalisation d'une analyse d'impact relative à la protection des données (AIPD). Les organismes pourront ainsi définir les mesures permettant d'assurer la proportionnalité et la nécessité de leurs traitements (points 3 à 7), de garantir les droits des personnes (points 8 et 9) et la maîtrise de leurs risques (point 10). À cette fin, l'organisme pourra se référer aux lignes directrices de la CNIL sur les analyses d'impact relatives à la protection des données (AIPD).

[1] Article 8 ou Article 17-II-2° de la loi n° 2016-1691 du 9 décembre 2016 relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique.
[2] Loi n° 2017-399 du 27 mars 2017 relative au devoir de vigilance des sociétés mères et des entreprises donneuses d'ordre.
[3] Article L. 4131-2 du code du travail.

3. Objectif(s) poursuivi(s) par le traitement (FINALITES)

Le traitement mis en œuvre doit répondre à un objectif précis et être justifié au regard des missions et des activités de l'organisme.

En ce qui concerne le dispositif d'alerte, le traitement de données est mis en œuvre afin de recueillir et traiter les alertes ou signalements visant à révéler un manquement à une règle spécifique.

Par exemple, un dispositif mis en œuvre pour répondre aux exigences de l'article 8 de la loi « Sapin 2 » vise à permettre de signaler :

- un crime ou délit ;
- une violation grave et manifeste d'un engagement international régulièrement ratifié ou approuvé par la France ;
- une violation grave et manifeste d'un acte unilatéral d'une organisation internationale pris sur le fondement d'un engagement international régulièrement ratifié ;
- une violation grave et manifeste de la loi ou du règlement ;
- une menace ou un préjudice graves pour l'intérêt général, dont l'émetteur de l'alerte a eu personnellement connaissance ;
- un manquement au code de conduite interne mis en œuvre dans l'organisme dans le cadre de la lutte contre la fraude et le trafic d'influence.

La loi « Sapin 2 » envisage divers dispositifs d'alerte interne qui peuvent être synthétisés dans le tableau suivant :

	Dispositif d'alerte (cas général)	Dispositif d'alerte interne (anticorruption)
Textes applicables	- **Articles 6 et suivants** de la loi n° 2016-1691 du 9 décembre 2016 - **Décret n° 2017-564 du 19 avril 2017** relatif aux procédures de recueil des signalements émis par les lanceurs d'alerte au sein des personnes morales de droit public ou de droit privé ou des administrations de l'Etat.	**Article 17, II, 2°** de la loi n° 2016-1691 du 9 décembre 2016, et recommandations de l'AFA prises en application de l'**article 3,2°** de la loi du 9 décembre 2016.
Organisations concernées	- les personnes morales de droit public ou de droit privé d'au moins cinquante salariés, - les administrations de l'Etat, - les communes de plus de 10 000 habitants, - les établissements publics de coopération intercommunale à fiscalité propre dont elles sont membres, - les départements et les régions, dans des conditions fixées par décret en Conseil d'Etat.	**Article 17** : les sociétés ou établissements publics à caractère industriel et commercial : - employant au moins **500 salariés** (ou appartenant à un groupe) et ; - dont le chiffre d'affaires ou le chiffre d'affaires consolidé est supérieur à **100 millions d'euros**. **Article 3,2°** : toutes les organisations exposées au risque de corruption.

Faits objets de l'alerte	- un crime ou un **délit,** - une violation grave et manifeste 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, de la loi ou du règlement, - une menace ou un préjudice graves pour l'intérêt général.	**Conduites ou situations contraires au code de conduit**e de l'organisation définissant et illustrant les différents types de comportements à proscrire comme étant susceptibles de caractériser des faits de corruption ou de trafic d'influence.
Lanceurs d'alerte	- les membres du personnel, - les collaborateurs extérieurs et occasionnels.	Employés de l'organisation.

Les informations recueillies pour l'une de ces finalités ne peuvent pas être réutilisées pour poursuivre un autre objectif qui serait incompatible avec la finalité première. Tout nouvel usage des données doit en effet respecter les principes de protection des données personnelles. Les traitements mis en œuvre ne doivent pas donner lieu à des interconnexions ou échanges autres que ceux nécessaires à l'accomplissement des finalités ci-dessus énoncées.

4. Base(s) légale(s) du traitement

Chaque finalité du traitement doit reposer sur l'une des « bases légales » fixées par la réglementation. Les différents fondements autorisant un organisme à traiter des données personnelles dans le cadre d'un dispositif d'alerte sont listés ci-dessous.

Dans le cadre du présent traitement, la base légale peut être :

a) **le respect d'une obligation légale incombant à l'organisme,** imposant la mise en œuvre d'un dispositif d'alerte ;

Il doit s'agir d'une disposition légale intégrée au corpus juridique français. Par exemple, la loi « Sapin 2 » contient une telle obligation légale en ce qu'elle impose à certains organismes de mettre en œuvre un dispositif visant à permettre le recueil d'alertes.

b) la réalisation de l'intérêt légitime poursuivi par l'organisme ou par le destinataire des données, sous réserve de ne pas méconnaître l'intérêt ou les droits et libertés fondamentaux de la personne concernée.

Lorsqu'un responsable de traitement décide de mettre en œuvre un tel dispositif sans y être obligé par la loi, alors le fondement légal de son traitement sera la réalisation de l'intérêt légitime.

5. Données personnelles concernées

5.1 Principe de pertinence, de loyauté et de minimisation des données.

Dans un souci de minimisation des données personnelles traitées, l'organisme doit veiller à ne collecter et utiliser que les données pertinentes et nécessaires au regard de ses propres besoins de traitement des signalements. Il peut s'agir des données relatives aux :

a) **identité, fonctions et coordonnées de l'émetteur de l'alerte professionnelle ;**

b) **identité, fonctions et coordonnées des personnes faisant l'objet d'une alerte ;**

c) **identité, fonctions et coordonnées des personnes intervenant dans le recueil ou dans le traitement de l'alerte ;**

d) **faits signalés ;**

e) **éléments recueillis dans le cadre de la vérification des faits signalés ;**

f) **comptes-rendus des opérations de vérification ;**

g) **suites données à l'alerte.**

Les faits recueillis sont strictement limités aux actes visés par le dispositif d'alerte. La prise en compte de l'alerte ne s'appuie que sur des données formulées de manière objective, en rapport direct avec le périmètre du dispositif d'alerte, et strictement nécessaires à la vérification des faits allégués. Les formulations utilisées pour décrire la nature des faits signalés font apparaître leur caractère présumé.

Certaines données, en raison de leur caractère particulièrement sensible, bénéficient d'une protection particulière et ne peuvent être traitées que dans des cas spécifiques.

Il s'agit notamment des :

- données sensibles, c'est-à-dire celles dont le traitement est en principe interdit sauf exception(s). Il s'agit des données qui révèlent l'origine prétendument raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale d'une personne, des données génétiques, des données biométriques utilisées aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne (article 9.1 RGPD) ;

- données relatives aux infractions, condamnations et mesures de sécurité concernant des personnes physiques.

Ces catégories de données ne peuvent être collectées et traitées que dans des conditions strictement définies. Dans le cadre du présent traitement, la collecte de ces données peut être autorisée :

- par des dispositions spécifiques du droit national ; ou

- pour permettre au responsable de traitement de préparer et, le cas échéant, d'exercer et de suivre une action en justice en tant que victime, mise en cause, ou pour le compte de ceux-ci.

5.2. Traitement de l'identité de l'auteur d'une alerte

Un dispositif d'alerte peut imposer ou proposer que l'auteur de l'alerte s'identifie.

Si l'émetteur de l'alerte professionnelle doit s'identifier, son identité est traitée de façon confidentielle par l'organisation chargée de la gestion des alertes.

Il est toutefois recommandé que l'organisme n'incite pas les personnes ayant vocation à utiliser le dispositif à le faire de manière anonyme, étant entendu qu'une alerte anonyme est une alerte dont l'auteur n'est ni identifié ni identifiable.

Par exception, l'alerte d'une personne qui souhaite rester anonyme devrait être traitée sous les conditions suivantes :

- la gravité des faits mentionnés est établie et les éléments factuels sont suffisamment détaillés ;
- le traitement de cette alerte doit s'entourer de précautions particulières, telles qu'un examen préalable, par son premier destinataire, de l'opportunité de sa diffusion dans le cadre du dispositif.

Après s'être assuré de la nécessité et de la pertinence des données personnelles qu'il utilise, l'organisme doit par ailleurs s'assurer, tout au long de la durée de vie du traitement, de la qualité des données qu'il traite. Cela signifie en pratique que conformément à la règlementation, les données soient exactes et mises à jour.

6. Destinataires des informations

Les données personnelles doivent uniquement être rendues accessibles aux personnes habilitées à en connaitre au regard de leurs attributions.

Les habilitations d'accès doivent être documentées par les organismes, et les accès aux différents traitements doivent faire l'objet de mesures de traçabilité. **Voir point 9 relatif à la sécurité.**

Le responsable de traitement qui souhaite avoir recours à un sous-traitant doit veiller à ne faire appel qu'à des organismes présentant des garanties suffisantes. Un contrat définissant les caractéristiques du traitement ainsi que les différentes obligations des parties en matière de protection des données doit être établi entre elles (article 28 du RGPD). Un guide du sous-traitant, édité par la CNIL, précise ces obligations et les clauses à intégrer dans les contrats.

6.1. Les personnes accédant aux données pour le compte de l'employeur

Seules les personnes habilitées au titre de leurs missions ou de leurs fonctions, doivent pouvoir accéder aux données à caractère personnel traitées, et ce dans la stricte limite de leurs attributions respectives et de l'accomplissement de ces missions et fonctions.

Il peut s'agir, par exemple :

- des personnes spécialement chargées de la gestion des alertes au sein de l'organisme ;
- du référent ou prestataire de service chargé de recueillir et traiter les alertes. Le référent ou prestataire de service éventuellement désigné pour gérer tout ou partie de ce dispositif s'engage notamment, par voie contractuelle, à ne pas utiliser les données à des fins autres que la gestion des alertes, à assurer leur confidentialité, à respecter la durée de conservation limitée des données et à procéder à la destruction ou à la restitution de tous les supports manuels ou informatisés de données à caractère personnel au terme de sa prestation.

6.2. Les destinataires des données

Le RGPD définit les destinataires comme « tout organisme qui reçoit la communication des données ».

Dans le cadre de ce traitement, les données peuvent être communiquées au sein du groupe de sociétés auquel appartient l'organisme concerné si cette communication est nécessaire aux seuls besoins de la vérification ou du traitement de l'alerte.

Certaines dispositions légales ou réglementaires encadrent strictement la communication d'information. Ainsi, les éléments de nature à identifier l'émetteur de l'alerte ne peuvent être divulgués, sauf à l'autorité judiciaire, qu'avec le consentement de la personne. De même, les éléments de nature à identifier la personne mise en cause par un signalement ne peuvent être divulgués, sauf à l'autorité judiciaire, qu'une fois établi le caractère fondé de l'alerte.

Pour assurer la continuité de la protection des données à caractère personnel, leur transfert en dehors de l'Union européenne est soumis à des règles particulières. Ainsi, conformément aux dispositions des articles 44 et suivants du RGPD, toute transmission de données hors de l'UE doit :

- être fondée sur une décision d'adéquation ;
- ou être encadrée par des règles internes d'entreprise (« BCR »), des clauses types de protection des données, un code de conduite ou un mécanisme de certification approuvé par la CNIL ;
- ou être encadrée par des clauses contractuelles ad hoc préalablement autorisées par la CNIL ;
- ou répondre à une des dérogations prévues à l'article 49 du RGPD.

Pour en savoir plus, consulter la rubrique « Transférer des données hors de l'UE » sur le site de la CNIL.

6. Durées de conservation

Une durée de conservation précise des données doit être fixée en fonction de chaque finalité : ces données ne peuvent être conservées pour une durée indéfinie.

Au regard des finalités pouvant justifier la mise en place d'un dispositif d'alerte, et sauf dispositions légales ou réglementaires contraires :

a) les données relatives à une alerte, considérées par le responsable du traitement comme n'entrant pas dans le champ du dispositif, sont soit détruites sans délai soit peuvent être conservées à la condition d'avoir été préalablement anonymisées à bref délai (voir les lignes directrices du CEPD sur l'anonymisation) ;

b) lorsque l'alerte n'est pas suivie d'une procédure disciplinaire ou judiciaire, les données relatives à cette alerte sont détruites ou archivées, après anonymisation à bref délai, par l'organisation chargée de la gestion des alertes dans un délai de deux mois à compter de la clôture des opérations de vérification ;

c) lorsqu'une procédure disciplinaire ou contentieuse est engagée à l'encontre de la personne mise en cause ou de l'auteur d'une alerte abusive, les données relatives à l'alerte sont conservées par l'organisation chargée de la gestion des alertes jusqu'au terme de la procédure et expiration des voies de recours, ou conservées au-delà après avoir été préalablement anonymisées à bref délai.

Si le choix de l'anonymisation des données est fait par l'organisme, il lui incombe la responsabilité de garantir le caractère anonymisé des données de façon pérenne.

Les données peuvent être conservées plus longtemps, en archivage intermédiaire, si le responsable du traitement en a l'obligation légale (par exemple, pour répondre à des obligations comptables, sociales ou fiscales) ou s'il souhaite se constituer une preuve en cas de contentieux et dans la limite du délai de prescription/forclusion applicable.

Pour en savoir plus, vous pouvez vous référer aux guides de la CNIL :

- « Sécurité : Archiver de manière sécurisée » ;
- « Limiter la conservation des données ».

Les données utilisées à des fins statistiques ne sont plus qualifiées de données à caractère personnel dès lors qu'elles auront ont été dûment anonymisées (Voir les lignes directrices du CEPD sur l'anonymisation).

Exemple : un organisme est soumis à l'obligation de mettre en place un dispositif d'alerte en application des dispositions de l'article 8 de la loi « Sapin 2 » (dispositif d'alerte général), mais également un dispositif d'alerte en application de l'article 17-II-2° de la même loi (dispositif visant à permettre le signalement de manquements ou situations contraires au code de conduite de l'organisme, dans le cadre de la lutte contre la corruption et le trafic d'influence).

Il est alors possible pour l'organisme de mettre en place un seul et unique outil de recueil de ces signalements. Toutefois, il peut exister des différences d'encadrement législatif et réglementaire des traitements. Ainsi, les modalités de mise en place des dispositifs d'alerte généraux sont encadrées, notamment en ce qui concerne les durées de conservation, par un décret.

Or, ce décret n'est pas applicable en matière de lutte contre la corruption et le trafic d'influence. Les données recueillies via les dispositifs spécifiques d'alerte ne font donc pas l'objet d'un encadrement particulier et leur traitement doit être encadré en application de la réglementation.

La mise en place d'un outil unique de recueil des signalements implique de respecter les exigences législatives et réglementaires de chacun des dispositifs, et notamment de :

- différencier le traitement appliqué aux signalements portant sur des soupçons ou des faits de corruption de celui appliqué aux autres signalements ;
- d'appliquer des durées de conservation différentes selon que les données sont collectées dans le cadre de l'un ou l'autre des dispositifs d'alerte ;
- de s'assurer que les dispositifs soient bien ouverts aux personnes concernées telles que les collaborateurs extérieurs et occasionnels, s'agissant du dispositif d'alerte général.
    - Les collaborateurs occasionnels sont les stagiaires qui, dans l'exercice de leurs fonctions, peuvent, à l'instar de salariés ou de fonctionnaires, avoir connaissance de risques ou de faits répréhensibles ;
    - Les collaborateurs extérieurs désignent les personnes qui, bien qu'employées par une entité autre que celle auprès ou pour le compte de laquelle elles exercent leurs fonctions, disposent d'une connaissance approfondie de cette dernière et peuvent avoir connaissance de faits répréhensibles.

Il s'agit donc d'une personne présentant un lien professionnel avec l'organisation (par exemple : intérimaires, consultants, sous-traitants, intermédiaires).

7. Information des personnes

Un traitement de données personnelles doit être mis en œuvre en toute transparence vis-à-vis des personnes concernées.

Ainsi, dès le stade de la collecte des données personnelles, les personnes doivent être informées des modalités de traitement de leurs données dans les conditions prévues par les articles 12, 13 et 14 du RGPD (Voir les modèles de mention d'information).

Les personnes concernées doivent par ailleurs être informées de la manière d'exercer leurs droits.
Les instances représentatives du personnel doivent également être informées et consultées conformément à la réglementation en vigueur.

7.1. Information générale au moment du déploiement du traitement

Au-delà de l'information collective et individuelle prévue par le code du travail, les personnes concernées doivent être informées dans les conditions prévues par l'article 13 du RGPD.

Le responsable de traitement doit délivrer une information claire et précise aux personnes susceptibles d'utiliser le dispositif, c'est-à-dire, le cas échéant, aux membres du personnel de l'organisme mais également aux tiers ayant vocation à utiliser le dispositif.

L'information précise notamment les étapes de la procédure de recueil des signalements, en particulier les destinataires et les conditions auxquelles l'alerte peut leur être adressée.

Il est recommandé que le responsable de traitement indique expressément que l'utilisation abusive du dispositif peut exposer son auteur à d'éventuelles sanctions ou poursuites mais qu'à l'inverse, l'utilisation de bonne foi du dispositif n'exposera son auteur à aucune sanction disciplinaire, quand bien même les faits s'avéreraient par la suite inexacts ou ne donneraient lieu à aucune suite.

Il est également recommandé au responsable de traitement de rappeler que le dispositif d'alerte n'est qu'un moyen de signalement parmi d'autres (au même titre que la voie hiérarchique), et que les membres du personnel ne peuvent pas être sanctionnés pour défaut de son utilisation.

7.2. Information spécifique de la personne visée par l'alerte

Par principe, le responsable de traitement doit informer la personne visée par une alerte dès l'enregistrement, informatisé ou non, de données la concernant afin de lui permettre de s'opposer au traitement de ces données.

Cette information, qui est réalisée selon des modalités permettant de s'assurer de sa bonne délivrance à la personne concernée, précise notamment l'entité responsable du dispositif, les faits qui lui sont reprochés, les services éventuellement destinataires de l'alerte ainsi que les modalités d'exercice de ses droits d'accès, d'opposition et de rectification.

Néanmoins, étant dans le cadre d'une collecte indirecte de données et en application des dispositions de l'article 14.5.b) du RGPD, des dérogations à ces modalités d'information peuvent être obtenues par le responsable de traitement dans le cas où l'information de la personne visée par l'alerte est susceptible « *de compromettre gravement la réalisation des objectifs dudit traitement* ». Tel pourrait notamment être le cas lorsque cette information compromettrait la prise de mesures conservatoires pour prévenir la destruction de preuves relatives à l'alerte.

Cette possibilité est néanmoins conditionnée à la prise de mesures appropriées pour protéger les droits et libertés ainsi que les intérêts légitimes de la personne concernée.
Au titre de ces mesures appropriées, dans le cadre d'un dispositif d'alerte, le responsable de traitement s'engage à informer la personne visée par l'alerte dans les modalités précédemment exposées, aussitôt après l'adoption de ces mesures conservatoires.

8. Droits des personnes

Les personnes concernées disposent des droits suivants, qu'ils exercent dans les conditions prévues par le RGPD (voir la rubrique qui s'intitule « respecter les droits des personnes » sur le site de la CNIL) :

- droit de **s'opposer au traitemen**t de leurs données, sous réserve des conditions d'exercice de ce droit en application des dispositions de l'article 21 du RGPD ;
- droit **d'accès, de rectification et d'effacement** des données qui les concernent ;
- droit à la **limitation** du traitement. Par exemple, lorsque la personne conteste l'exactitude de ses données, celle-ci peut demander à l'organisme, le gel temporaire du traitement de ses données, le temps que celui-ci procède aux vérifications nécessaires.

8.1. Principes généraux

Le RGPD reconnait un certain nombre de droits aux personnes dès lors que leurs données à caractère personnel font l'objet d'un traitement. Ces droits sont distincts de ceux pouvant naitre au profit de ces mêmes personnes dans le cadre du procès civil ou pénal (par exemple les droits de la défense, le respect du principe du contradictoire, etc.).

De par leur situation à l'égard des dispositifs d'alerte, toutes les personnes concernées peuvent être classées en trois grandes catégories :

- celles qui émettent l'alerte ;
- celles qui font l'objet d'une alerte en tant qu'auteurs présumés des faits ;
- celles qui font l'objet d'une alerte en tant que victimes ou témoins présumés des faits.

L'étendue et les modalités d'exercice des droits ne seront pas nécessairement identiques pour chacune de ces catégories, du fait de la différence de leur situation à l'égard du traitement de leurs données.

Enfin, il est à noter que le choix d'une base légale du traitement conditionne l'existence de certains droits. Ainsi, un dispositif identique déployé dans deux organismes différents mais fondé sur deux bases légales distinctes, ne créera pas nécessairement les mêmes droits au profit des personnes concernées.

8.2. Droit d'accès

Lorsque les personnes concernées exercent leur droit d'accès, elles ne peuvent *via* l'exercice de ce droit, obtenir communication d'aucune donnée relative à des tiers.

La personne visée par l'alerte qui exercerait son droit d'accès **ne peut en aucun cas obtenir communication des informations concernant l'identité de l'émetteur de l'alerte**.

8.3. Droit d'opposition, de rectification, de suppression

Si le dispositif d'alerte est mis en œuvre par l'organisme pour répondre à une obligation légale, la base légale du traitement est celle prévue par l'article 6-1-c du RGPD, à savoir la nécessité d'exécuter cette obligation. La personne concernée par une alerte ne peut alors pas s'opposer par principe au traitement de ses données personnelles, conformément aux dispositions de l'article 21 du RGPD.

En revanche, si le responsable de traitement décide de lui-même de mettre en œuvre un dispositif d'alerte sans qu'il n'y soit contraint par la loi, la base légale du traitement est l'intérêt légitime poursuivi par le responsable de traitement (article 6-1 f) du RGPD). La personne concernée disposera alors d'un droit d'opposition pour des raisons tenant à sa situation particulière, sur le fondement du même article 21.

La personne visée par l'alerte ne peut exercer son droit d'opposition au seul prétexte qu'elle ne souhaite pas figurer dans ce traitement. Toutefois, elle pourrait s'opposer au traitement de ses données personnelles en cas d'erreur, en prouvant que ses données n'ont pas ou plus à être traitées.

9. Sécurité

L'organisme doit prendre toutes les précautions utiles au regard des risques présentés par son traitement pour préserver la sécurité des données à caractère personnel et, notamment au moment de leur collecte, durant leur transmission et leur conservation, empêcher qu'elles soient déformées, endommagées ou que des tiers non autorisés y aient accès.

En particulier, dans le contexte spécifique du présent référentiel, **soit l'organisme adopte les mesures suivantes, soit il justifie de leur équivalence ou du fait de ne pas avoir besoin ou pouvoir y recourir** :

Catégories	Mesures
Sensibiliser les utilisateurs	Informer et sensibiliser les personnes manipulant les données
	Rédiger une charte informatique et lui donner une force contraignante
Authentifier les utilisateurs	Définir un identifiant (*login*) unique à chaque utilisateur
	Adopter une politique de mot de passe utilisateur conforme aux recommandations de la CNIL
	Obliger l'utilisateur à changer son mot de passe après réinitialisation
	Limiter le nombre de tentatives d'accès à un compte
Gérer les habilitations	Définir des profils d'habilitation
	Supprimer les permissions d'accès obsolètes
	Réaliser une revue annuelle des habilitations
Tracer les accès et gérer les incidents	Prévoir un système de journalisation
	Informer les utilisateurs de la mise en place du système de journalisation
	Protéger les équipements de journalisation et les informations journalisées
	Prévoir les procédures pour les notifications de violation de données à caractère personnel
Sécuriser les postes de travail	Prévoir une procédure de verrouillage automatique de session
	Utiliser des antivirus régulièrement mis à jour
	Installer un « pare-feu » (*firewall*) logiciel
	Recueillir l'accord de l'utilisateur avant toute intervention sur son poste
Sécuriser l'informatique mobile	Prévoir des moyens de chiffrement des équipements mobiles
	Faire des sauvegardes ou des synchronisations régulières des données
	Exiger un secret pour le déverrouillage des *smartphones*
Protéger le réseau informatique interne	Limiter les flux réseau au strict nécessaire
	Sécuriser les accès distants des appareils informatiques nomades par VPN
	Mettre en œuvre le protocole WPA2 ou WPA2-PSK pour les réseaux Wi-Fi
Sécuriser les serveurs	Limiter l'accès aux outils et interfaces d'administration aux seules personnes habilitées
	Installer sans délai les mises à jour critiques
	Assurer une disponibilité des données
Sécuriser les sites web	Utiliser le protocole TLS et vérifier sa mise en œuvre
	Vérifier qu'aucun mot de passe ou identifiant n'est transmis dans les URL
	Contrôler que les entrées des utilisateurs correspondent à ce qui est attendu
	Mettre un bandeau de consentement pour les *cookies* non nécessaires au service
Sauvegarder et prévoir la continuité d'activité	Effectuer des sauvegardes régulières
	Stocker les supports de sauvegarde dans un endroit sûr
	Prévoir des moyens de sécurité pour le convoyage des sauvegardes
	Prévoir et tester régulièrement la continuité d'activité
Archiver de manière	Mettre en œuvre des modalités d'accès spécifiques aux données archivées

Catégories	Mesures
sécurisée	Détruire les archives obsolètes de manière sécurisée
Encadrer la maintenance et la destruction des données	Enregistrer les interventions de maintenance dans une main courante
	Encadrer par un responsable de l'organisme les interventions par des tiers
	Effacer les données de tout matériel avant sa mise au rebut
Gérer la sous-traitance	Prévoir une clause spécifique dans les contrats des sous-traitants
	Prévoir les conditions de restitution et de destruction des données
	S'assurer de l'effectivité des garanties prévues (audits de sécurité, visites, *etc.*)
Sécuriser les échanges avec d'autres organismes	Chiffrer les données avant leur envoi
	S'assurer qu'il s'agit du bon destinataire
	Transmettre le secret lors d'un envoi distinct et via un canal différent
Protéger les locaux	Restreindre les accès aux locaux au moyen de portes verrouillées
	Installer des alarmes anti-intrusion et les vérifier périodiquement
Encadrer les développements informatiques	Proposer des paramètres respectueux de la vie privée aux utilisateurs finaux
	Éviter les zones de commentaires ou les encadrer strictement
	Tester sur des données fictives ou anonymisées
Utiliser des fonctions cryptographiques	Utiliser des algorithmes, des logiciels et des bibliothèques reconnues
	Conserver les secrets et les clés cryptographiques de manière sécurisée

Pour ce faire, le responsable de traitement pourra utilement se référer au Guide de la sécurité des données personnelles

10. Analyse d'impact sur la protection des données (AIPD)

En application des dispositions de l'article 35 du RGPD, **le responsable de traitement peut avoir à réaliser une analyse d'impact** dès lors que son traitement de données présenterait un risque élevé pour les droits et les libertés des personnes.

Pour l'appréciation de ces risques, il conviendra de se référer aux critères établis par le Comité européen de la protection des données (CEPD) dans les lignes directrices concernant l'analyse d'impact relative à la protection des données (AIPD) et la manière de déterminer si le traitement est « susceptible d'engendrer un risque élevé », ainsi qu'à la liste adoptée par la CNIL, des types d'opérations de traitement pour lesquelles une analyse d'impact relative à la protection des données est requise.

Sur la base de ces critères, la mise en œuvre d'un traitement de données dans le cadre d'un dispositif d'alerte nécessite de réaliser une AIPD dans la mesure où ce traitement présente un risque élevé pour les droits et libertés des personnes concernées en ce qu'il :

- peut concerner des personnes considérées comme **vulnérables** (salariés) ;
- peut entraîner la **collecte de données sensibles ou à caractère hautement personnel** (données relatives à des infractions) ;
- est susceptible de produire **des effets juridiques à l'égard des personnes concernées** (par exemple des mesures disciplinaires pouvant aller jusqu'au licenciement).

Les risques les plus importants présentés par ce dispositif sont :

- **pour le lanceur d'alerte** : le risque de subir des représailles, des discriminations ou de voir prononcées à son encontre des mesures disciplinaires pour avoir dénoncé les faits ;

- **pour la personne visée par l'alerte** : le risque de subir des dénonciations calomnieuses (et leurs conséquences), de voir prononcées à son encontre des mesures disciplinaires sur le seul fondement des faits signalés, sans que leur véracité n'ait été examinée.

Pour réaliser une étude d'impact, le responsable de traitement pourra se reporter :
- aux principes contenus dans ce référentiel ;
- aux outils méthodologiques proposés par la CNIL sur son site web.

Si l'organisme en a désigné, le délégué à la protection des données (DPD/DPO) devra être consulté.

Conformément à l'article 36 du RGPD, le responsable de traitement doit consulter la CNIL préalablement à la mise en œuvre du traitement si l'analyse d'impact indique qu'il ne parvient pas à identifier des mesures suffisantes pour réduire les risques à un niveau acceptable.