LE CONTRÔLEUR EUROPÉEN DE LA PROTECTION DES DONNÉES (CEPD)

Lignes directrices relatives au traitement d'informations à caractère personnel dans le cadre d'une procédure d'alerte éthique

Décembre 2019

Résumé

Les procédures d'alerte éthique servent à révéler des actes répréhensibles ou des actes de corruption. L'un des grands défis, pour prévenir la corruption, réside dans la détection et la mise au jour des pots-de-vin, fraudes, vols et autres actes répréhensibles commis sur le lieu de travail. L'alerte éthique permet d'exposer au grand jour des comportements contraires à l'éthique de ce type.

Les lanceurs d'alerte étant susceptibles de faire l'objet de représailles sous la forme de harcèlement, d'un licenciement, d'une mise sur liste noire, de menaces et/ou de tout bonnement voir leurs révélations ignorées, la loi leur offre une protection. La confidentialité, notamment par la protection de l'anonymat, est donc un moyen essentiel et efficace d'encourager les membres du personnel à faire part de leurs préoccupations.

Les présentes lignes directrices fournissent des orientations pratiques aux institutions et organes de l'UE, tant avant qu'après l'exécution d'une procédure d'alerte éthique, afin de s'assurer qu'ils respectent les obligations en matière de protection des données établies par le règlement (CE) 2018/1725.

Les présentes lignes directrices sont une mise à jour des lignes directrices sur l'alerte éthique publiées en juillet 2016.

Liste des recommandations

Ci-dessous figure une liste des recommandations détaillées plus avant dans les lignes directrices. Le Contrôleur européen de la protection des données (CEPD) s'en servira comme liste de contrôle pour évaluer votre respect des obligations énoncées dans le règlement.

1. Établir des filières spécifiques pour la soumission de rapports internes et externes ainsi que des règles spécifiques dont la finalité est clairement indiquée (p. 5).

2. Assurer la confidentialité des informations reçues et protéger l'identité des lanceurs d'alerte ainsi que de toutes les autres personnes impliquées (p. 5).

3. Appliquer le principe de minimisation des données: ne traiter que les informations à caractère personnel adéquates, pertinentes et non excessives pour l'affaire en cause (p. 6-7).

4. Déterminer ce que veut dire «information à caractère personnel» dans ce contexte ainsi que l'identité des personnes concernées, afin d'établir leur droit d'information, d'accès et de rectification. Ces droits peuvent être limités pour autant que les institutions de l'UE soient en mesure de motiver au préalable leur décision (p. 7).

5. Appliquer la procédure en deux étapes afin d'informer chaque catégorie de personnes de la manière dont leurs données seront traitées (p. 7-8).

6. Veiller, lors des réponses aux demandes relatives au droit d'accès, à ce qu'aucune information personnelle d'une autre partie ne soit divulguée (p. 9-10).

7. S'assurer de la compétence du destinataire (interne ou externe), puis limiter le transfert d'informations à caractère personnel à ce qui est strictement nécessaire à l'exécution légitime des missions relevant de la compétence du destinataire (p. 10).

8. Définir des périodes de conservation adéquates pour les informations à caractère personnel traitées dans le cadre de la procédure d'alerte éthique, en fonction de l'issue de chaque cas (p. 10-11).

9. Mettre en œuvre des mesures de sécurité organisationnelles et techniques, basées sur une analyse du risque de la procédure d'alerte éthique, afin de garantir le traitement sûr et licite des informations à caractère personnel (p. 11-12).

TABLE DES MATIÈRES

1. INTRODUCTION

1 Les procédures d'alerte éthique visent à fournir des filières sûres permettant à toute personne de signaler les cas potentiels de fraudes, corruption et autres manquements et irrégularités graves dont elle a connaissance. Les procédures d'alerte éthique protègent les lanceurs d'alerte et les divulgations qui sont dans l'intérêt public. Les procédures d'alerte éthique ne visent pas à signaler un grief ou à déposer une plainte.

2 Les présentes lignes directrices ont pour but de fournir aux institutions et organes de l'Union européenne (IUE) des conseils et instructions pratiques sur le traitement des données à caractère personnel dans le cadre de leur procédure d'alerte éthique, pour s'assurer qu'ils respectent leurs obligations en matière de protection des données telles qu'énoncées dans le règlement (UE) 2018/1725[1] (ci-après le «règlement»).

3 Le CEPD a élaboré les présentes lignes directrices à la lumière de sa longue expérience. Une première édition en a été publiée en juillet 2016; entre-temps, de nouvelles règles de protection des données applicables aux IUE ont remplacé le règlement (CE) nº 45/2001. Le nouveau règlement reflète le règlement général sur la protection des données (RGPD) applicable aux organisations de l'UE/EEE. En outre, une nouvelle directive sur la protection des personnes qui dénoncent des infractions au droit de l'Union[2] (la «directive») a été adoptée[3]. Les présentes lignes directrices ont été mises à jour afin de tenir compte du règlement actuel ainsi que de certains éléments de la directive, même si elle n'est pas applicable aux institutions de l'UE.

4 Le statut des fonctionnaires (le «statut») et le régime applicable aux autres agents (le «RAA»)[4] prévoient des obligations spécifiques, pour les membres du personnel et les autres personnes qui travaillent pour les IUE, de signaler par écrit toute suspicion raisonnable d'activités illégales à leur hiérarchie ou directement à l'Office européen de lutte antifraude («OLAF»). Des IUE se sont en outre dotées de règles internes sur le lancement d'alertes éthiques par leur personnel. Les dispositifs d'alerte éthique servant de mécanisme de détection lui-même destiné à signaler les cas d'activités illégales à l'OLAF, l'obligation d'information ne concerne que les manquements et irrégularités graves. La portée des présentes lignes directrices se limite à l'étape initiale à laquelle les IUE reçoivent une notification et ne couvre pas les cas où l'affaire est renvoyée vers l'OLAF ou directement transmise à celui-ci.

5 Les procédures d'alerte éthique prévoient le traitement de catégories particulières de données. Les IUE sont tenues de gérer les rapports d'alerte et de veiller à la protection des informations à caractère personnel des lanceurs d'alerte, des présumés coupables, des témoins et de toutes les personnes apparaissant dans le rapport. Les présentes lignes directrices expliquent comment appliquer les principes relatifs à la protection des données

[1] JO L 295 du 21.11.2018, p. 39.
[2] DIRECTIVE DU PARLEMENT EUROPÉEN ET DU CONSEIL relative à la protection des personnes dénonçant les infractions au droit de l'Union, 2018/0106 (COD).
[3] La législation va maintenant être officiellement signée et publiée au Journal officiel.
[4] Le cadre juridique général applicable aux membres du personnel de l'UE agissant en tant que lanceurs d'alerte est établi aux articles 22 *bis*, 22 *ter* et 22 *quater* du statut, qui, conformément à l'article 11 du régime applicable aux autres agents de l'UE, s'appliquent par analogie aux agents engagés par contrat.

à ce contexte, susceptible d'affecter la vie privée d'individus. Ces explications sont illustrées par une série d'exemples hypothétiques. Les lignes directrices montrent également que les principes relatifs à la protection des données peuvent servir à renforcer les procédures d'alerte éthique. L'application des principes relatifs à la protection des données favorisera ainsi la création de filières sûres en renforçant les aspects de la procédure liés à la sécurité.

6 Les parties externes qui concluent un contrat avec les IUE ou qui prennent contact avec celles-ci (p. ex. consultants, contractants, chercheurs, etc.) doivent être informées de la possibilité de signaler les suspicions de fraude, de corruption ou d'autres manquements et irrégularités graves.

2. DES FILIÈRES DE COMMUNICATION SÉCURISÉES POUR LE SIGNALEMENT DES FRAUDES - GARANTIR LA CONFIDENTIALITÉ

7 La manière la plus efficace d'inciter les membres du personnel à signaler des problèmes est de faire en sorte que leur identité soit protégée. C'est pourquoi des filières de communication clairement définies pour les signalements internes et externes et la protection des informations reçues doivent être créées. L'identité du lanceur d'alerte signalant des manquements ou irrégularités graves en toute bonne foi doit être traitée avec la plus grande confidentialité afin de protéger le lanceur d'alerte contre d'éventuelles représailles. Son identité ne peut en aucun cas être révélée, hormis dans des circonstances exceptionnelles, s'il en autorise la divulgation, si cette dernière est requise par une procédure de droit pénal ultérieure ou lorsque le lanceur d'alerte fait une fausse déclaration par malveillance. Dans de tels cas, ces données à caractère personnel ne pourraient être divulguées qu'aux autorités judiciaires[5]. Une déclaration est effectuée par malveillance si le lanceur d'alerte signale des activités qu'il sait être inventées. Si une IUE apprend qu'un lanceur d'alerte a formulé des allégations non étayées, il incombe à l'institution de prouver le caractère malveillant des allégations.

8 La personne visée par une allégation doit être protégée au même titre que le lanceur d'alerte en raison du risque de stigmatisation et de victimisation de la personne au sein de l'organisation dont elle est membre. La personne sera exposée à ces risques avant même de savoir qu'elle a été mise en cause et avant même que les faits allégués aient fait l'objet d'une enquête pour déterminer s'ils sont fondés ou non.

9 Les rapports d'alerte peuvent également inclure des renseignements personnels concernant des tiers, tels que des témoins ou des collègues. Ces informations devraient également être protégées à tous les stades de la procédure[6].

10 Dès lors, l'accès en interne aux informations traitées dans le cadre de l'enquête sur les allégations doit être accordé sur la stricte base du principe du besoin d'en connaître, autrement dit, s'il existe une nécessité d'y accéder. Les personnes responsables de la gestion des rapports peuvent par exemple être soumises à une obligation de confidentialité

[5] Voir CEPD, dossier 2010-0458.
[6] Considérant 76 de la directive.

renforcée. Les informations à caractère personnel doivent également être stockées en toute sécurité.

11 Toute information à caractère personnel en rapport avec une alerte éthique et conservée à des fins statistiques doit être rendue anonyme. Les IUE (en particulier les plus petites) doivent être particulièrement prudentes avec les informations susceptibles de permettre une identification indirecte. Par exemple, enregistrer le type d'alerte éthique au même endroit que la nationalité du lanceur d'alerte pourrait entraîner l'identification indirecte de ce dernier et doit donc être évité.

Exemple 1: *une agence de l'UE a adressé des recommandations explicites à son personnel sur la manière d'assurer la confidentialité des lanceurs d'alerte et des auteurs présumés lors de l'examen initial d'une affaire. Le CEPD souligne que la vulnérabilité des parties impliquées est la même, que l'affaire soit en cours ou qu'elle soit close. La protection des lanceurs d'alerte et des auteurs présumés doit par conséquent être également prise en compte une fois l'affaire close.*

3. ÉVITER TOUT ABUS DE LA PROCÉDURE - SPÉCIFIER LA FINALITÉ

12 Le champ d'application de la procédure doit être limité afin d'éviter tout abus de la procédure. La finalité de la procédure d'alerte éthique doit être **clairement spécifiée**[7] dans le règlement interne ou la politique des IUE. Le règlement interne ou la politique doit décrire expressément les circonstances dans lesquelles les filières de communication réservées aux alertes éthiques doivent être utilisées et les circonstances dans lesquelles elles ne doivent pas l'être. En règle générale, les filières de communication réservées aux alertes éthiques **ne doivent pas être utilisées** lorsque le membre du personnel pourrait souhaiter exercer ses droits légaux, à savoir introduire une demande ou une plainte auprès de l'autorité investie du pouvoir de nomination en vertu de l'article 90 du statut ou lorsqu'il s'agit d'un cas de harcèlement ou d'un différend personnel, auquel cas le membre du personnel peut s'adresser aux RH, au service de médiation ou à un conseiller qui respectera le principe de confidentialité, ou encore introduire une demande d'assistance au titre de l'article 24 du statut.

13 Le règlement intérieur ou la politique doit par ailleurs décrire que les informations sensibles, telles que l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale ainsi que les données relatives à la santé ou à la vie sexuelle[8], sont dénuées de pertinence pour l'affaire et doivent être évitées. Cela contribuera à éviter la collecte d'informations à caractère personnel excessives (voir section 4 ci-dessous).

14 En principe, **l'alerte éthique ne devrait pas être anonyme**. Les lanceurs d'alerte devraient être invités à s'identifier, non seulement pour éviter tout abus de la procédure, mais aussi pour permettre leur protection efficace contre d'éventuelles représailles. Cela

[7] Article 4, paragraphe 1, point b), du règlement.
[8] Article 10, paragraphe 1, du règlement.

permettra également une meilleure gestion du dossier s'il est nécessaire de recueillir des informations supplémentaires.

4. ÉVITER LE TRAITEMENT D'INFORMATIONS À CARACTÈRE PERSONNEL EXCESSIVES

15 Les IUE entrent parfois en possession d'informations à caractère personnel manifestement dénuées de tout intérêt ou de pertinence au regard des allégations. **Les informations de ce type ne doivent pas faire l'objet d'un traitement ultérieur.** Cette exigence est particulièrement importante pour certaines catégories d'informations. Tous les agents chargés de l'examen des allégations doivent être informés de cette règle.

Exemple 2: *un lanceur d'alerte signale qu'un de ses collègues a commis une fraude. Dans le cadre de sa déclaration, il se retrouve à divulguer des informations sur l'état de santé de son collègue. Il est clair, pour l'institution, que cette information est dénuée de toute pertinence au regard de l'activité frauduleuse signalée et qu'elle ne doit donc ni faire l'objet d'un traitement ultérieur, ni être renvoyée à son expéditeur.*

16 Une bonne pratique consiste à mettre en œuvre une recommandation générale, par exemple dans le règlement intérieur, pour ceux qui traitent des fichiers d'alerte éthique afin de leur rappeler de respecter les règles de qualité des données.[9] Une autre bonne pratique, telle que précisée dans la directive[10], consisterait à dispenser une formation en matière de protection des données aux membres du personnel responsables du traitement des demandes.

5. DÉTERMINER CE QUE LES TERMES «INFORMATIONS À CARACTÈRE PERSONNEL» SIGNIFIENT DANS CE CONTEXTE

17 Les données à caractère personnel sont définies comme toute information concernant une personne physique identifiée ou identifiable[11]. Les informations à caractère personnel n'incluent pas seulement les informations relatives à la vie privée et familiale d'une personne, mais aussi les informations concernant ses activités, telles que ses relations professionnelles ou son comportement économique et social[12]. Il convient de prendre en compte ces éléments lors de la détermination de la portée du droit d'accès de la personne concernée, par exemple. La plupart du temps, les informations à caractère personnel incluent des données d'identification (par exemple, des coordonnées), mais aussi des données relatives au comportement de la personne.

[9] Article 4, paragraphe 1, du règlement.
[10] Considérant 74 de la directive.
[11] Article 3, paragraphe 1, du règlement.
[12] Groupe de travail «Article 29», avis 4/2007 sur le concept de données à caractère personnel, WP 136, adopté le 20 juin 2007.

Exemple 3: *le rapport du lanceur d'alerte inclut des informations identifiant l'auteur présumé et des témoins. Il contient également des informations personnelles sur le lanceur d'alerte, puisqu'il concerne son propre comportement (en tant que lanceur d'alerte).*

18 Une même information peut concerner plusieurs individus en même temps. Le rapport du lanceur d'alerte peut contenir des informations à caractère personnel sur les témoins et tierces parties (des personnes uniquement citées dans le dossier), les personnes à l'encontre desquelles les allégations sont portées et le lanceur d'alerte lui-même.

19 Par contre, le seul fait qu'un nom soit mentionné dans un document ne fait pas nécessairement de toutes les informations qui y figurent des «données relatives à cette personne». Dans bon nombre de cas, une information ne peut être considérée comme «relative à» un individu que si elle concerne celui-ci.

Exemple 4: *une institution de l'UE rédige un rapport dans lequel elle examine la pertinence d'un renvoi de l'affaire devant l'OLAF. Dans son analyse, elle peut faire référence au lanceur d'alerte en tant que source, mais le rapport n'est pas entièrement constitué d'informations à caractère personnel sur le lanceur d'alerte.*

6. INFORMER CHAQUE CATÉGORIE DE PERSONNES

20 Des informations sur les procédures d'alerte éthique doivent être fournies aux personnes concernées de façon très visible, ce qui nécessite une procédure en **deux temps**. Si l'affichage d'un avis relatif à la protection des données sur le site web (ou sur un document public ou interne) est encouragé, le CEPD considère qu'il **ne suffit pas** en l'espèce, car les informations ne seront pas forcément lues. Un avis relatif à la protection des données devrait également être mis le plus rapidement possible à la disposition de toutes les personnes impliquées dans une procédure d'alerte éthique, par exemple par courrier électronique. Les personnes concernées sont en général les lanceurs d'alerte, les témoins, des tierces parties (des membres du personnel ou d'autres personnes uniquement citées) ainsi que la ou les personnes visées par les allégations.

6.1 Information du lanceur d'alerte (article 15 du règlement)

21 Dans ce contexte, il est important d'indiquer à toutes les personnes associées à la procédure l'identité des personnes avec qui leurs informations à caractère personnel vont être partagées (destinataires potentiels ou catégories de destinataires[13]). L'avis relatif à la protection des données doit également informer les personnes des conséquences d'une utilisation abusive (si le lanceur d'alerte effectue une fausse déclaration par malveillance, par exemple) de la procédure d'alerte éthique (p. ex. des mesures disciplinaires).

[13] Article 15, paragraphe 1, point d), du règlement

6.2 Informations fournies à l'auteur présumé (article 16 du règlement)

22 Dans certains cas, informer la personne à l'encontre de laquelle une allégation a été portée à un stade précoce de la procédure peut compromettre le bon déroulement de celle-ci. Dans ce type de cas, il peut être nécessaire de limiter le partage de certaines informations spécifiques[14]. Les IUE doivent disposer de règles internes pour pouvoir restreindre les informations (voir paragraphe 26 ci-dessous). Le report de l'information devrait être décidé au cas par cas. Les raisons des éventuelles limitations devraient être documentées et mises à la disposition du CEPD s'il en fait la demande dans le cadre d'une mesure de surveillance et d'application. Ces raisons doivent démontrer, par exemple, l'existence d'un risque élevé que l'accès aux informations nuise à la procédure ou aux droits et libertés des autres personnes. Les raisons doivent être documentées avant l'adoption de la décision relative à d'éventuelles limitations ou à un renvoi.

6.3 Information des témoins (article 15 du règlement)

23 Des informations spécifiques doivent être fournies aux témoins dans les plus brefs délais, par exemple avant qu'ils soient interrogés par l'institution.

6.4 Information des tierces parties (article 16 du règlement)

24 Selon le cas particulier, l'information de toutes les tierces parties mentionnées dans un rapport d'alerte éthique peut supposer un effort disproportionné[15]. Il convient de déterminer au cas par cas si l'information des tierces parties est disproportionnée. Par ailleurs, dans certains cas, l'information des personnes représenterait un traitement supplémentaire potentiellement plus intrusif que le premier.

Exemple 5:
a) un lanceur d'alerte joint à son rapport une liste des clients (200 personnes) d'un hôtel afin de prouver que l'auteur présumé se trouvait à l'hôtel à une date donnée. Les 199 autres clients n'ont aucun lien avec l'affaire et leurs informations ne font pas l'objet d'un traitement ultérieur par l'institution. Il n'est pas nécessaire de les informer.
b) Un lanceur d'alerte joint à son rapport une clé USB contenant des échanges de courriers électroniques avec l'auteur présumé et quelques autres membres du personnel. L'institution effectue un examen préliminaire et traite les informations relatives aux autres membres du personnel. Il convient alors d'en informer ceux-ci.

[14] Article 25 du règlement.
[15] Article 16, paragraphe 5, point b), du règlement.

7. ÉVALUER LE DROIT D'ACCÈS ET LES LIMITATIONS DE L'ACCÈS DE LA PERSONNE

25 Lorsqu'elles examinent les droits d'accès, les IUE doivent tenir compte du statut du demandeur et de l'état actuel[16] de l'enquête. Le niveau et la sensibilité des informations détenues (ainsi que tout éventuel risque associé à leur divulgation) varient en fonction de l'auteur de la demande:

- la personne visée par une allégation;
- le lanceur d'alerte;
- un témoin;
- une tierce partie.

26 Les IUE doivent veiller à ce qu'il existe une base juridique claire avant de mettre en œuvre toute limitation en vertu de l'article 25 du règlement. Cela signifie que les IUE doivent avoir adopté des règles internes couvrant les cas exceptionnels où des informations pourraient être reportées. En outre, avant de mettre en œuvre une restriction dans un cas spécifique, un test de nécessité et de proportionnalité doit être effectué et les IUE doivent documenter les motifs de leur décision afin d'être responsables. Pour plus d'informations sur les règles internes et l'évaluation au cas par cas, veuillez consulter les orientations du CEPD concernant l'article 25 du nouveau règlement et les règles internes. En outre, les IUE pourraient devoir faire la distinction entre une justification interne de l'utilisation de la limitation et une justification générale à communiquer au demandeur en vertu de l'article 25, paragraphe 6, à moins que ces informations ne puissent être reportées en vertu de l'article 25, paragraphe 8.

Exemple 6: *un lanceur d'alerte (A) signale une fraude présumée de la part d'un collègue et supérieur (B). Une fois l'enquête terminée, B demande l'accès à ses données à caractère personnel traitées à cet effet. Certaines parties des allégations formulées par A sont considérées comme des données à caractère personnel de B. L'IUE pourrait être en mesure de justifier une limitation au titre de l'article 25, paragraphe 1, point h), concernant le fait que A a fourni les données, et si l'on pouvait supposer que c'est A qui a fourni ces informations, A pourrait faire l'objet de représailles de la part de B. Cela devrait être documenté en interne. De toute évidence, B ne doit pas être informé que la raison de la limitation réside dans le fait que A pourrait subir des représailles, car cela viderait la limitation de tout effet conformément à l'article 25, paragraphe 8. Par conséquent, les informations communiquées à B en vertu de l'article 25, paragraphe 6, devraient être formulées de manière plus générale.*

[16] Voir article 25, paragraphe 1, points a) et b), du règlement.

27 **Lorsque l'accès aux informations personnelles d'un individu est accordé, les informations à caractère personnel de tierces parties telles que des informateurs, des lanceurs d'alerte ou des témoins doivent être effacées des documents, sauf dans des circonstances exceptionnelles,** si le lanceur d'alerte consent à cette divulgation, pour les besoins d'une éventuelle procédure pénale[17] ultérieure ou en cas de fausse déclaration du lanceur d'alerte effectuée par malveillance. Si un risque d'identification de tierces parties subsiste, l'accès doit être reporté. La directive prévoit une obligation de confidentialité (article 16, paragraphe 1), les États membres étant tenus de veiller à ce que l'identité de la personne déclarante ne soit divulguée à personne en dehors des membres du personnel autorisés sans le consentement explicite de cette personne. Cette recommandation est particulièrement importante si l'on veut faire en sorte que les individus soient protégés contre tous les risques potentiels inhérents à la divulgation de leurs informations à caractère personnel.

Exemple 7: *un employé de l'UE accusé de manquements graves demande à l'institution toutes les informations à caractère personnel le concernant en rapport avec les accusations. La plupart de ces informations figurent dans les témoignages du lanceur d'alerte. Même si le nom de celui-ci est effacé des documents, son identité serait évidente au vu des références aux évènements, situations et contextes spécifiques qui y sont décrits. L'institution doit donc reporter la publication de ces informations pour garantir la protection de la personne concernée ou des droits et libertés d'autrui [article 25, paragraphe 1, point h), pour autant que cela soit établi dans les règles internes de l'IUE].*

8. LIMITER LES TRANSFERTS

28 Des obligations différentes s'appliquent selon que le destinataire est une IUE (dans ce contexte, lorsqu'une institution transfère des données à l'OLAF) ou un destinataire soumis au RGPD (comme une juridiction nationale ou un autre type de destinataire)[18]. **La nécessité de ce transfert de données doit être déterminée au cas par cas.** En particulier, le transfert de données à caractère personnel n'est justifié que lorsqu'il est nécessaire à l'exécution légitime des missions relevant de la compétence du destinataire.

9. ÉTABLIR DES PÉRIODES DE CONSERVATION EN FONCTION DE L'ISSUE DE L'AFFAIRE

29 Les informations à caractère personnel peuvent uniquement être conservées pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités du traitement[19]. Il convient donc de fixer différentes périodes de conservation en fonction des informations incluses dans le rapport et de la manière dont l'affaire est traitée:

[17] Article 16, paragraphe 2, de la directive: l'identité peut être divulguée *«[...] uniquement lorsqu'il s'agit d'une obligation nécessaire et proportionnée imposée par le droit de l'Union ou le droit national dans le cadre d'enquêtes menées par des autorités nationales ou dans le cadre de procédures judiciaires, notamment en vue de sauvegarder les droits de la défense de la personne concernée»*.
[18] Article 9 du règlement.
[19] Article 4, paragraphe 1, point e), du règlement.

30 Les informations à caractère personnel qui sont dénuées de pertinence au regard des allégations ne devraient pas faire l'objet d'un traitement ultérieur (voir section 4) et devraient être supprimées sans tarder[20].

31 Si après examen initial, il apparaît clairement que l'affaire ne devrait pas être renvoyée devant l'OLAF ou qu'elle ne relève pas de la procédure d'alerte éthique, le rapport doit être supprimé dans les plus brefs délais (ou renvoyé vers la bonne filière s'il porte par exemple sur une accusation de harcèlement). En tout état de cause, les informations à caractère personnel devraient être supprimées rapidement et généralement dans un délai de deux mois à compter de l'aboutissement de l'examen préliminaire[21], vu que la conservation de telles informations sensibles serait excessive.

32 S'il apparaît nécessaire, à l'issue de l'examen initial, de transférer le rapport à l'OLAF, l'IUE doit rester attentive aux mesures que l'OLAF décide de prendre. Si l'OLAF ouvre une enquête, il n'est pas nécessaire que l'IUE conserve plus longtemps les informations. Si l'OLAF décide de ne pas ouvrir d'enquête, les informations doivent être effacées sans délai.

33 Dans le cas où une période de conservation plus longue serait envisagée, l'accès aux informations à caractère personnel doit tout de même être limité (voir les mesures de sécurité ci-dessous). Il est de bonne pratique de conserver ces rapports à l'écart du principal système de gestion des dossiers/système quotidien utilisé.

Exemple 8: *une institution de l'UE a reçu plusieurs rapports d'alerte éthique par le biais de sa filière d'alerte. L'un d'entre eux concerne une accusation de harcèlement et est donc directement renvoyé vers l'unité responsable de ces affaires. Deux autres pourraient porter sur des cas de fraude et sont donc transférés à l'OLAF, qui ouvre une enquête sur l'un des cas. L'institution applique une période de conservation de cinq ans en ce qui concerne les dossiers sur lesquels l'OLAF n'ouvre pas d'enquête. Dans cette situation, le CEPD estime qu'une période de cinq ans est excessive et que le rapport devrait être supprimé le plus tôt possible.*

10. METTRE EN ŒUVRE DES MESURES DE SÉCURITÉ ADÉQUATES

34 L'IUE (ou le responsable du traitement des données, à savoir l'entité qui détermine les finalités et moyens applicables au traitement des données à caractère personnel) doit mettre en œuvre les mesures techniques et organisationnelles appropriées pour assurer un niveau de sécurité adéquat au regard des risques présentés par le traitement et de la nature des données à caractère personnel à protéger[22]. La confidentialité constitue une obligation légale claire et est un élément important pour encourager le personnel à signaler toute préoccupation qu'il pourrait avoir. Les mesures de sécurité doivent en outre prendre en considération le caractère sensible des informations personnelles traitées. Il est essentiel, dans ce contexte, de mettre en place des mesures de sécurité adéquates afin d'empêcher efficacement des personnes non autorisées d'accéder aux informations à caractère personnel et de garantir l'intégrité de celles-ci.

[20] Article 17 de la directive, dernière phrase.
[21] Avis 1/2006 du groupe de travail «article 29», WP 117, p. 12.
[22] Article 33 du règlement.

35 **La nécessité de ces mesures de sécurité doit être analysée à la lumière des risques inhérents à la procédure d'alerte éthique, sous la forme d'une évaluation des risques de sécurité de l'information manuelle ou automatique.** Une fois que les risques pour les informations à caractère personnel concernées ont été déterminés, une nouvelle analyse peut être effectuée afin de déterminer les mesures à mettre en œuvre, en tenant également compte du coût de ces mesures de sécurité et de leur viabilité. Les risques évoluant au fil du temps, il est nécessaire que l'IUE réexamine régulièrement son analyse, la sélection des mesures de sécurité ainsi que l'efficacité de celles-ci.

36 Des orientations détaillées sur la gestion des risques de sécurité de l'information sont proposées dans le document «Guidance on Security Measures for Personal Data Processing - Article 22 of Regulation 45/2001» du CEPD (à actualiser).

Exemple 9: *en particulier lorsqu'il s'agit de dossiers d'alerte éthique,*
a) le personnel autorisé à avoir accès aux informations à caractère personnel doit être strictement limité en fonction du principe du besoin d'en connaître. Le personnel autorisé doit être soumis à une obligation de confidentialité renforcée et l'accès aux rapports d'alerte éthique doit être contrôlé, qu'il se fasse sous forme électronique ou sur papier.
b) Du point de vue technique, les exigences relatives au contrôle de l'accès doivent être pleinement appliquées, à savoir limiter et contrôler efficacement les personnes autorisées à accéder aux dossiers d'alerte éthique, consulter les journaux et réexaminer régulièrement l'accès aux journaux et les droits d'accès.
c) Vu l'importance d'assurer une stricte confidentialité de ces informations, il convient d'envisager notamment le recours au chiffrement. Même en cas de chiffrement, des mécanismes de garantie doivent être mis en œuvre afin de permettre l'accès aux informations en cas de besoin (partage de clés, enregistrement et conservation sécurisée des mots de passe, etc.)

11. VEILLEZ À POUVOIR RENDRE DES COMPTES!

37 L'obligation de rendre des comptes signifie que les IUE doivent respecter leurs obligations en matière de protection des données et **être en mesure de démontrer qu'elles le font**. (Article 4, paragraphe 2, et article 26 du règlement)

38 Cette notion n'est pas propre aux informations à caractère personnel concernées par une procédure d'alerte éthique, mais s'applique à toutes les opérations de traitement d'informations à caractère personnel.

39 Toute IUE qui collecte, utilise et stocke (ce que l'on appelle collectivement le traitement) des informations à caractère personnel est responsable du respect des règles en matière de protection des données et doit pouvoir rendre des comptes à cet égard.

40 D'une manière générale, les IUE doivent faire preuve de transparence et être explicites quant à la manière dont elles traitent les informations à caractère personnel liées aux procédures d'alerte éthique. Elles doivent documenter leurs politiques et veiller à ce que les utilisateurs en aient connaissance. Le droit au respect de la vie privée et à la protection des données existe sur le lieu de travail également et tout le monde doit en être informé. Les IUE ne peuvent pas partir du principe que le personnel est au courant. (Article 14 du règlement)

41 Le meilleur moyen pour une institution de pouvoir rendre des comptes consiste à examiner les implications des nouveaux processus du point de vue de la protection des données dès le stade de la conception (**protection des données dès la conception**), article 27 du règlement. Les différents traitements et les différentes technologies exigent des garanties différentes. S'il est associé dès le début du processus, le délégué à la protection des données (DPD) pourra apporter des conseils et des orientations utiles.

42 Les questions figurant ci-après exposent les principaux points à prendre en considération:

a. **Confidentialité:** comment protégez-vous les personnes concernées?

b. **Déterminer la finalité:** quand utiliser la filière d'alerte éthique?

c. **Éviter les informations excessives:** Quelles informations sont nécessaires dans le contexte des allégations formulées?

d. **Définir le terme «informations à caractère personnel»:** qu'est-ce qu'une information à caractère personnel dans ce rapport particulier?

e. **Informer chaque catégorie de personnes:** Qui est concerné par l'alerte éthique?

f. **Appliquer différentes périodes de conservation:** combien de temps dois-je conserver le rapport?

g. **Effectuer une évaluation des risques pour la sécurité des informations:** Quels sont les risques potentiels pour la sécurité des informations à caractère personnel contenues dans les alertes éthiques et comment comptez-vous atténuer ces risques?

43 Pour démontrer la responsabilité, la procédure et sa mise en œuvre doivent être documentées. Les documents suivants sont requis:

a. **une politique, un règlement interne ou une décision** sur l'alerte éthique,

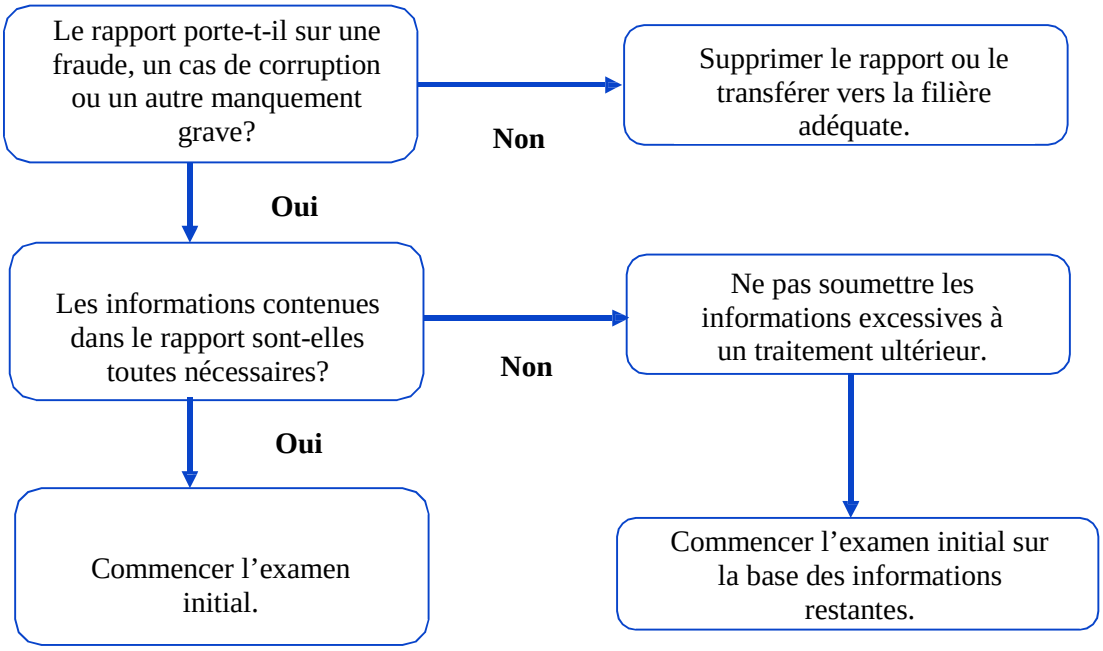
b. **les limitations à certains droits des personnes concernées** (incluses dans les règles internes des IUE), les motifs sur lesquels reposent les limitations et le raisonnement justifiant l'application de ces limitations,

c. tout **report d'informations** à la personne concernée (conformément aux règles internes),

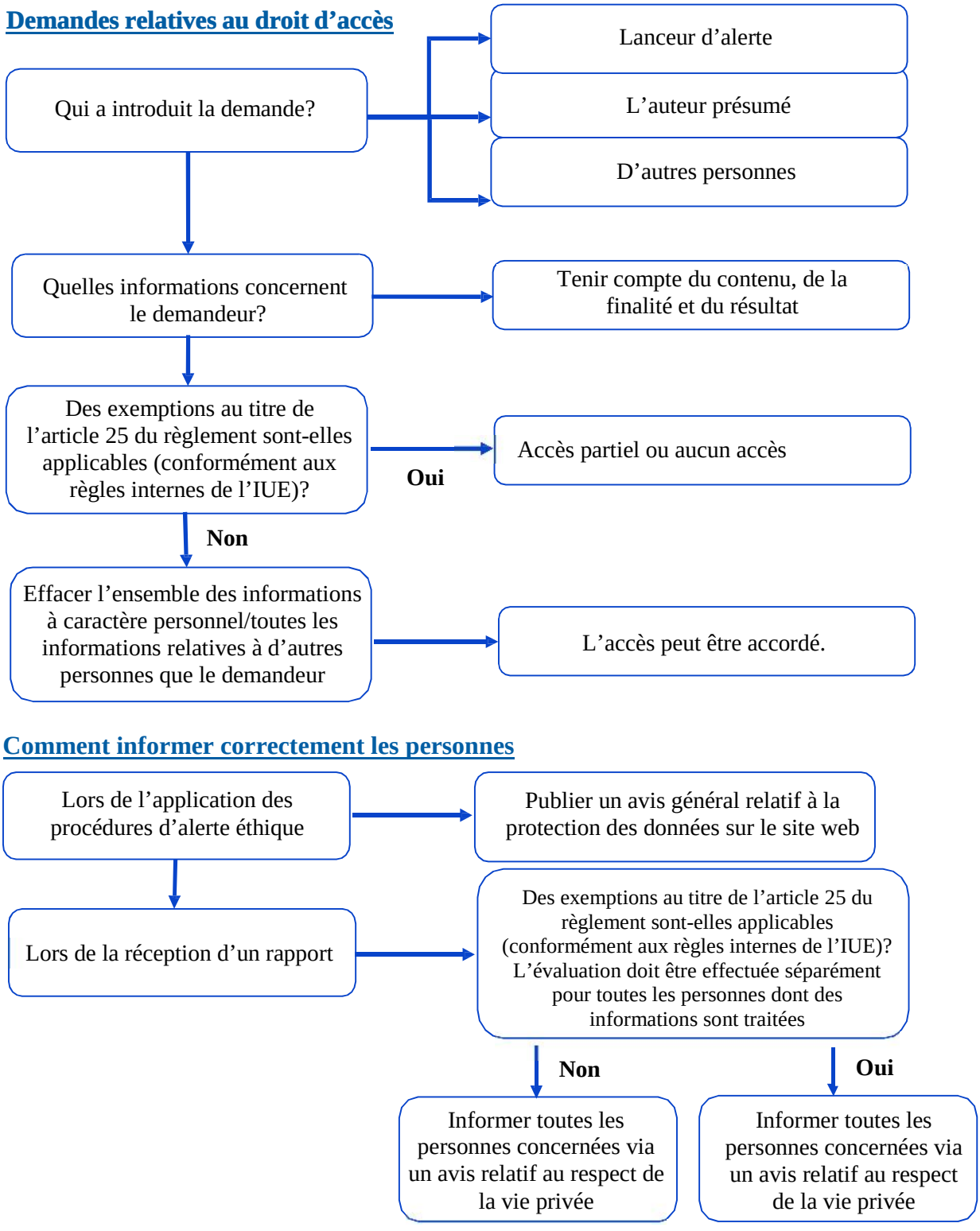
d. l'**évaluation des risques** effectuée pour la procédure en question.

12. ORGANIGRAMMES DES PROCÉDURES D'ALERTE ÉTHIQUE

12.1 Gestion des rapports d'alerte éthique



12.2 Garantir le respect des droits des personnes



LECTURES COMPLÉMENTAIRES

La directive sur la protection des personnes qui signalent des violations du droit de l'Union

Exemples d'avis du CEPD

2016-1083 –- Avis sur les procédures internes et les lignes directrices de l'OEDT en matière d'alerte éthique

2015-0061 - Avis du CEPD sur la procédure de l'Agence exécutive du Conseil européen de la recherche relative au traitement interne et au signalement d'éventuelles fraudes et irrégularités

2015-0349 – Avis sur la procédure d'alerte éthique du Secrétariat général du Conseil de l'Union européenne

2015-0569 – Avis sur la procédure de transmission d'informations de l'Agence européenne de contrôle des pêches

2014-0828 – Avis sur la procédure d'alerte éthique du Médiateur européen