Commission nationale de l'informatique et des libertés

Délibération n° 2017-191 du 22 juin 2017 portant modification de la délibération n° 2005-305 du 8 décembre 2005 portant autorisation unique de traitements automatisés de données à caractère personnel mis en œuvre dans le cadre de dispositifs d'alerte professionnelle (AU-004) (rectificatif)

NOR : *CNIL1721434Z*

Rectificatif au *Journal officiel* du 25 juillet 2017, texte n° 61.

La délibération 2017-191 du 22 juin 2017 est modifiée comme suit :

Vu la Convention n° 108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ;

Vu la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement de données à caractère personnel et la libre circulation de ces données ;

Vu la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifiée par la loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, et notamment son article 25-I-3°, 25-I-4° et 25-II ;

Vu 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 ;

Vu le 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 ;

Vu la délibération n° 2005-305 du 8 décembre 2005 portant autorisation unique de traitements automatisés de données à caractère personnel mis en œuvre dans le cadre de dispositifs d'alerte professionnelle ;

Vu la délibération n° 2010-369 du 14 octobre 2010 modifiant l'autorisation unique n° 2005-305 du 8 décembre 2005 n° AU-004 ;

Vu la délibération n° 2014-042 du 30 janvier 2014 modifiant l'autorisation unique n° 2010-369 du 14 octobre 2010 n° AU-004 ;

Vu le document d'orientation relatif aux dispositifs d'alerte professionnelle adopté par la Commission le 10 novembre 2005, annexé à la présente décision ;

Après avoir entendu Mme Marie-France MAZARS, commissaire, en son rapport, et Mme Nacima BELKACEM, commissaire du Gouvernement, en ses observations,

Emet l'avis suivant :

Un dispositif d'alerte professionnelle est un système mis en œuvre par des organismes publics ou privés, à destination des membres de leur personnel ou des collaborateurs extérieurs et occasionnels pour les inciter à signaler à l'organisme employeur des comportements, dont ils ont eu personnellement connaissance, qu'ils estiment contraires aux règles applicables, et pour organiser la vérification de l'alerte ainsi recueillie au sein de l'organisme concerné.

Ce dispositif est mis en œuvre complémentairement aux voies traditionnelles de signalement et son utilisation ne constitue qu'une faculté pour l'employé de l'organisme.

Les dispositifs d'alerte professionnelle mis en œuvre sur les lieux de travail peuvent prendre la forme de traitements automatisés de données à caractère personnel susceptibles, du fait de leur portée, d'exclure des personnes du bénéfice de leur contrat de travail en l'absence de toute disposition législative ou réglementaire et susceptibles également de contenir des données relatives à des infractions.

Dès lors, de tels dispositifs constituent des traitements relevant tant de l'article 25-I 3° que de l'article 25-I-4° de la loi du 6 janvier 1978 modifiée et doivent, à ce titre, être autorisés par la CNIL.

En vertu de l'article 25-II de la loi du 6 janvier 1978 modifiée, la Commission peut adopter une décision unique d'autorisation pour des traitements répondant notamment aux mêmes finalités, portant sur des catégories de données et des catégories de destinataires identiques.

Le responsable de traitement mettant en œuvre un dispositif d'alerte professionnelle dans le respect des dispositions de cette décision unique adresse à la Commission un engagement de conformité à la présente autorisation.

La Commission décide que les responsables de traitement qui lui adressent une déclaration comportant un engagement de conformité pour leurs traitements de données à caractère personnel répondant aux conditions fixées par la présente décision unique sont autorisés à mettre en œuvre ces traitements.

Art. 1er. – *Finalités du traitement*

Peuvent faire l'objet d'un engagement de conformité à la présente décision unique, les traitements automatisés de données à caractère personnel mis en œuvre par les organismes publics ou privés ayant pour finalité le signalement et le traitement des alertes, émises par une personne physique, relatives à :

– un crime ou un 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 ;
– ou une menace ou un préjudice graves pour l'intérêt général, dont l'émetteur de l'alerte a eu personnellement connaissance.

Sont également couverts par la présente décision unique, les traitements automatisés de données à caractère personnel mis en œuvre par un organisme pour le recueil de signalements, émanant de ses personnels, relatifs aux obligations définies par les règlements européens et par le code monétaire ou financier ou le règlement général de l'Autorité des marchés financiers et dont la surveillance est assurée par l'Autorité des marchés financiers ou l'Autorité de contrôle prudentiel et de résolution.

Sont également couverts par la présente décision unique, les traitements automatisés de données à caractère personnel mis en œuvre par un organisme pour le recueil de signalements, émanant d'employés, relatifs à l'existence de conduites ou de situations contraires au code de conduite de la société, concernant des faits de corruption ou de trafic d'influence, ce, dès lors que la mise en œuvre de ces traitements répond à une obligation légale ou à un intérêt légitime du responsable de traitement.

L'alerte ne peut toutefois pas porter sur des éléments couverts par le secret de la défense nationale, le secret médical ou le secret des relations entre un avocat et son client.

Art. 2. – *Traitement de l'identité de l'émetteur de l'alerte et de la personne visée*

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

L'organisme ne doit pas inciter les personnes ayant vocation à utiliser le dispositif à le faire de manière anonyme.

Par exception, l'alerte d'une personne qui souhaite rester anonyme peut 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.

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.

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.

Art. 3. – *Catégories de données à caractère personnel enregistrées*

Seules les catégories de données suivantes peuvent être traitées :

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

Les faits recueillis sont strictement limités aux actes visés par le dispositif d'alerte. La prise en compte de l'alerte professionnelle 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.

Art. 4. – *Destinataires des données à caractère personnel*

Sauf disposition légale ou règlementaire contraire, les signalements sont adressés au supérieur hiérarchique direct ou indirect, à l'employeur ou au référent désigné par lui. Ceux-ci ne sont destinataires de tout ou partie des données visées à l'article 4 que dans la mesure où ces données sont nécessaires à l'accomplissement de leurs missions.

Ces données peuvent être communiquées aux personnes spécialement chargées de la gestion des alertes professionnelles 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.

S'il est fait recours à un référent ou prestataire de service pour recueillir ou traiter les alertes, les personnes spécialement chargées de ces missions au sein de cet organisme n'accèdent à tout ou partie des données visées à

l'article 3 que dans la limite de leurs attributions respectives. 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 détournées, 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.

Dans tous les cas, les personnes chargées du recueil et du traitement des alertes professionnelles sont en nombre limité, spécialement formées et astreintes à une obligation renforcée de confidentialité contractuellement définie.

Art. 5. – *Transferts de données à caractère personnel hors de l'Union européenne*

Le présent article s'applique dans les cas où les communications de données envisagées à l'article 4 concernent un transfert vers une personne morale établie dans un pays non membre de l'Union européenne n'accordant pas une protection suffisante au sens de l'article 68 de la loi du 6 janvier 1978 modifiée.

Dans ces cas, ces communications de données à caractère personnel doivent s'opérer conformément aux dispositions spécifiques de la loi du 6 janvier 1978 modifiée relatives aux transferts internationaux de données, et notamment son article 69 alinéa 8.

Il est satisfait à ces dispositions lorsque la personne morale au sein de laquelle travaille le destinataire des données a adhéré au *Privacy Shield*, dans la mesure où la société étasunienne concernée a expressément fait le choix d'inclure les données de ressources humaines dans le champ de cette adhésion.

Il est également satisfait à ces dispositions lorsque le destinataire a conclu un contrat de transfert basé sur les clauses contractuelles types émises par la Commission européenne dans ses décisions du 15 juin 2001, du 27 décembre 2004, ou lorsque le groupe auquel appartiennent les entités concernés ont adopté des règles internes dont la CNIL a préalablement reconnu qu'elles garantissent un niveau de protection suffisant de la vie privée et des droits fondamentaux des personnes. S'il est satisfait à ces conditions, et si le traitement dont le transfert est issu est par ailleurs conforme à l'ensemble des autres dispositions de la présente délibération, la présente délibération porte également autorisation du transfert envisagé en application de l'article 69, alinéa 8, de la loi du 6 janvier 1978 modifiée.

Art. 6. – *Durée de conservation des données à caractère personnel*

Les données relatives à une alerte considérée, dès son recueil par le responsable du traitement, comme n'entrant pas dans le champ du dispositif sont détruites ou archivées sans délai, après anonymisation.

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, par l'organisation chargée de la gestion des alertes dans un délai de deux mois à compter de la clôture des opérations de vérification.

Lorsqu'une procédure disciplinaire ou des poursuites judiciaires sont engagées 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.

Les données faisant l'objet de mesures d'archivage sont conservées, dans le cadre d'un système d'information distinct à accès restreint, pour une durée n'excédant pas les délais de procédures contentieuses.

Art. 7. – *Mesures de sécurité*

Le responsable des traitements prend toutes précautions utiles pour préserver la sécurité des données tant à l'occasion de leur recueil que de leur communication ou de leur conservation.

En particulier, les accès aux traitements de données s'effectuent par un identifiant et un mot de passe individuels, régulièrement renouvelés, ou par tout autre moyen d'authentification. Ces accès sont enregistrés et leur régularité est contrôlée.

L'identité de l'émetteur d'une alerte et des personnes visées par l'alerte ainsi que les informations recueillies par l'ensemble des destinataires du signalement sont traitées de façon confidentielle.

Art. 8. – *Information des utilisateurs potentiels du dispositif*

Une information claire et complète de l'ensemble des utilisateurs potentiels du dispositif d'alerte est réalisée. Ainsi, cette information est délivrée aux membres du personnel de l'organisme mais également aux collaborateurs extérieurs et occasionnels ayant vocation à utiliser le dispositif.

Au-delà de l'information collective et individuelle prévue par le Code du travail, et conformément à l'article 32 de la loi du 6 janvier 1978 modifiée, cette information précise notamment l'identification de l'entité responsable du dispositif, les objectifs poursuivis et les domaines concernés par les alertes, le caractère facultatif du dispositif, l'absence de conséquence à l'égard des employés de la non-utilisation de ce dispositif, les éventuels transferts de données à caractère personnel à destination d'un Etat non membre de la Communauté européenne, ainsi que l'existence d'un droit d'accès, de rectification et d'opposition au bénéfice des personnes identifiées dans le cadre de ce dispositif.

L'information précise également les étapes de la procédure de recueil des signalements et notamment les destinataires et les conditions auxquelles l'alerte peut leur être adressée, conformément aux dispositions de l'article 8 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.

Il est clairement indiqué 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, même si les faits s'avèrent par la suite inexacts ou ne donnent lieu à aucune suite, n'exposera son auteur à aucune sanction disciplinaire.

Art. 9. – *Information de la personne faisant l'objet d'une alerte professionnelle*

La personne qui fait l'objet d'une alerte est, conformément aux articles 6 et 32 de loi du 6 janvier 1978, informée par le responsable du dispositif dès l'enregistrement, informatisé ou non, de données la concernant afin de lui permettre de s'opposer au traitement de ces données.

Lorsque des mesures conservatoires sont nécessaires, notamment pour prévenir la destruction de preuves relatives à l'alerte, l'information de cette personne intervient après l'adoption de ces mesures.

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 sont reprochés, les services éventuellement destinataires de l'alerte ainsi que les modalités d'exercice de ses droits d'accès et de rectification. Si elle n'en a pas bénéficié auparavant, la personne reçoit également une information conforme à l'article 8 de la présente décision.

Art. 10. – *Respect des droits d'accès et de rectification*

Conformément aux articles 39 et 40 de la loi du 6 janvier 1978 modifiée, le responsable du dispositif d'alerte garantit à toute personne identifiée dans le dispositif d'alerte professionnelle le droit d'accéder aux données la concernant et d'en demander, si elles sont inexactes, incomplètes, équivoques ou périmées, la rectification ou la suppression.

La personne qui fait l'objet d'une alerte ne peut en aucun cas obtenir communication du responsable du traitement, sur le fondement de son droit d'accès, des informations concernant l'identité de l'émetteur de l'alerte.

Art. 11. – Tout dispositif d'alerte professionnelle prévoyant la mise en œuvre de traitement de données à caractère personnel ne répondant pas aux dispositions précédentes doit faire l'objet d'une demande d'autorisation auprès de la Commission dans les formes prescrites par les articles 25-I 3° 25-I-4° et 30 de la loi du 6 janvier 1978 modifiée.

La présente délibération abroge et remplace la délibération n° 2005-305 du 8 décembre 2005 modifiée en dernier lieu le 30 janvier 2014 et sera publiée au *Journal officiel* de la République française.

La présidente,
I. Falque-Pierrotin