DECLARATION

17/11/2019

AU 4
Dispositif d’alertes professionnelles

DISPOSITIF D'ALERTES PROFESSIONNELLES

(Déclaration N° 4)

Suite à l'entrée en application du RGPD, les autorisations uniques adoptées par la CNIL n'ont plus de valeur juridique à compter du 25 mai 2018. Dans l'attente de la production de référentiels RGPD, la CNIL a décidé de les maintenir accessibles afin de permettre aux responsables de traitement d'orienter leurs premières actions de mise en conformité.

L'autorisation unique AU-004 a pour objectif d'encadrer les dispositifs d'alertes professionnelles en conformité avec les dispositions 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 dite « Loi Sapin II ».

Le champ de l'AU-004 est délimité non plus par rapport aux domaines concernés par les alertes mais par rapport à la nature des manquements signalés.

Sont exclues du champ de cette autorisation les alertes portant sur des faits couverts par le secret de la défense nationale, par le secret médical et par le secret des relations entre un avocat et son client.

TEXTE OFFICIEL

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)

SECTEURS D'ACTIVITE EXCLUS DU CHAMP DE LA NORME

Sont exclues du champ de cette autorisation les alertes portant sur des faits couverts par le secret de la défense nationale, par le secret médical et par le secret des relations entre un avocat et son client.

RESPONSABLES DE TRAITEMENT CONCERNES

Organismes publics ou privés mettant en œuvre un dispositif d'alertes professionnelles

OBJECTIF(S) POURSUIVI(S) PAR LE TRAITEMENT (FINALITES)

Peuvent faire l'objet d'un engagement de conformité à l'AU-004, les traitements automatisés de données à caractère personnel ayant pour finalité le traitement des alertes, émises par un membre du personnel ou un collaborateur extérieur et occasionnel, 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 ;

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.

UTILISATION(S) EXCLUE(S) DU CHAMP DE LA NORME

- Alertes portant sur des faits couverts par le secret de la défense nationale ;
- Alertes portant sur des faits couverts par le secret médical ;
- Alertes portant sur des faits couverts par le secret des relations entre un avocat et son client.

DONNEES PERSONNELLES CONCERNEES

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.

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.

Par exception, une alerte anonyme devra 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.

DONNEES EXCLUES DU CHAMP DE LA NORME

Toute information qui ne serait pas pertinente dans le cadre du traitement d'une alerte professionnelle

DUREE DE CONSERVATION DES DONNEES

- Lorsqu'une alerte est considérée comme n'entrant pas dans le champ du dispositif dès son recueil par le responsable de traitement, les données la concernant doivent immédiatement être supprimées ou archivées après anonymisation.
- Lorsqu'une alerte n'est pas suivie d'une procédure disciplinaire ou judiciaire, la suppression ou l'archivage après anonymisation doit intervenir dans un délai de deux mois après la clôture des vérifications, dans les conditions détaillées par la délibération.
- 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 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.

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.

DESTINATAIRES DES DONNEES

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.

Ces derniers ne doivent être destinataires que des seules données nécessaires à l'accomplissement de leurs missions.

Dans les limites de leurs attributions, peuvent également accéder aux données :

- les personnes spécialement chargées de la gestion des alertes professionnelles au sein du groupe de sociétés auquel appartient l'organisme concerné dès lors que 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.

Il appartient au responsable de traitement, avant chaque transmission de données, d'opérer un tri parmi ces dernières pour s'assurer que le destinataire accède aux seules données strictement nécessaires et proportionnées au regard de la justification de la communication.

INFORMATION DES PERSONNES ET RESPECT DES DROITS "INFORMATIQUE ET LIBERTES"

Information des utilisateurs potentiels du dispositif :

Une information est délivrée aux membres du personnel et 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 la loi « Informatique et Libertés », 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 la loi Sapin II.

Il est clairement indiqué que :

- l'utilisation abusive du dispositif peut exposer son auteur à des sanctions disciplinaires ainsi qu'à des poursuites judiciaires ;
- 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.

Information de la personne visée par l'alerte :

Outre l'information visée ci-dessus, la personne qui fait l'objet d'une alerte est 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.

SECURITE ET CONFIDENTIALITE

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.

TRANSFERTS DES DONNES HORS DE L'UNION EUROPEENNE

Il est possible de réaliser des transferts de données :

- vers un pays reconnu par une décision de la Commission européenne comme assurant un niveau de protection suffisant ;
- ou garantissant un niveau suffisant de protection de la vie privée, ainsi que les droits et libertés fondamentaux des personnes, par la mise en œuvre des clauses contractuelles types adoptées par la Commission européenne, ou par l'adoption de règles internes d'entreprise (BCR) ;
- ou lorsque la personne morale au sein de laquelle travaille le destinataire des données a adhéré au Bouclier de Protection des données (« *Privacy Shield*, ») dans la mesure où la société américaine concernée a expressément fait le choix d'inclure les données de ressources humaines dans le champ de cette adhésion
- ou justifiés par l'exception du 3° de l'article 69 de la loi du 6 janvier 1978 modifiée, c'est-à-dire le respect d'obligations permettant d'assurer la constatation, l'exercice ou la défense d'un droit en justice.

Le recours aux exceptions prévues par l'article 69 de la loi du 6 janvier 1978 modifiée n'est pas possible pour les transferts répétitifs, massifs ou structurels de données qui doivent quant à eux faire l'objet d'un encadrement spécifique (BCR ou clauses contractuelles types).