

Commission nationale de l'informatique et des libertés

Délibération n° 2014-042 du 30 janvier 2014 modifiant l'autorisation unique n° 2005-305 du 8 décembre 2005 n° AU-004 relative aux traitements automatisés de données à caractère personnel mis en œuvre dans le cadre de dispositifs d'alerte professionnelle

NOR : CNIX1403184X

La Commission nationale de l'informatique et des libertés,

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 des données à caractère personnel et à la libre circulation de ces données ;

Vu la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, notamment son article 25 (I, 4°) et 25-II ;

Vu le décret n° 2005-1309 du 20 octobre 2005 modifié pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ;

Vu la délibération n° 2005-305 du 8 décembre 2005 telle que modifiée par la délibération n° 2010-369 du 14 octobre 2010 ;

Après avoir entendu M. Emmanuel de GIVRY, commissaire, en son rapport et M. Jean-Alexandre SILVY, commissaire du Gouvernement, en ses observations,

Formule les observations suivantes :

La commission a adopté le 8 décembre 2005 une délibération portant autorisation unique (AU-004) de traitements automatisés de données à caractère personnel mis en œuvre dans le cadre de dispositifs d'alerte professionnelle (« *whistleblowing* »).

Cette autorisation unique a déjà été modifiée le 14 octobre 2010, notamment s'agissant du champ d'application des dispositifs d'alerte, qui avait été élargi à de nouveaux domaines.

Pour pouvoir faire l'objet d'un engagement de conformité à l'AU-004, les traitements de données à caractère personnel mis en œuvre doivent répondre aux exigences de l'article 1^{er} de l'autorisation unique, à savoir :

- soit répondre à une obligation législative ou réglementaire de droit français visant à l'établissement de procédures de contrôle interne dans les domaines financier, comptable, bancaire et de la lutte contre la corruption ;
- soit répondre à l'intérêt légitime du responsable du traitement au sens de l'article 7 (5°) de la loi du 6 janvier 1978 modifiée, ce dernier étant limité dans l'autorisation unique aux traitements mis en œuvre :
 - dans les domaines précités par les entreprises concernées par la section 301 (4) de la loi américaine dite « Sarbanes-Oxley » du 31 juillet 2002 ainsi que par la loi japonaise « Financial Instrument and Exchange Act » du 6 juin 2006 dite « Japanese SOX » ;
 - pour lutter contre les pratiques anticoncurrentielles au sein de l'organisme concerné.

La commission a relevé depuis que les dispositifs d'alerte professionnelle pour lesquels elle était saisie n'entraient pas dans le champ d'application de l'AU-004 ainsi défini.

Ces dispositifs, qui ont pu être autorisés spécifiquement par la commission, portent principalement sur la lutte contre les discriminations et le harcèlement au travail et plus généralement divers domaines mentionnés dans les codes éthiques (hygiène, santé et sécurité au travail, prévention des atteintes à l'environnement, protection des actifs de la société, conflits d'intérêt, confidentialité et données personnelles).

Dans ce contexte, il est apparu nécessaire à la commission de simplifier les formalités préalables en élargissant le champ d'application de l'AU-004 aux domaines de la lutte contre les discriminations et du harcèlement, de la santé, de l'hygiène et de la sécurité au travail ainsi que de la protection de l'environnement.

En effet, la mise en œuvre de dispositifs d'alerte dans ces domaines se justifie par le fait que les responsables de traitements ont l'obligation (au sens de l'article 7 [1°] de la loi du 6 janvier 1978 modifiée) ou un intérêt légitime (au sens de l'article 7 [5°] de la loi du 6 janvier 1978 modifiée) à mettre en place de tels traitements de données à caractère personnel qui répondent à des dispositions législatives, réglementaires ou conventionnelles de droit français ou étranger.

Les dispositifs d'alerte qui concernent d'autres domaines devront faire l'objet de demandes d'autorisations spécifiques.

La commission a également estimé nécessaire de clarifier les garanties relatives au traitement des alertes anonymes.

Compte tenu des réglementations étrangères, notamment de la loi Sarbannes-Oxley américaine, qui imposent aux entreprises situées en France de mettre en place un dispositif d'alerte professionnelle permettant de traiter les alertes anonymes, la commission a estimé que le recueil de ces alertes doit nécessairement être toléré dans les conditions qu'elle définit à l'article 2 de l'AU-004.

Dans ces conditions, la commission décide :

Art. 1^{er}. – L'article 1^{er} de la délibération n° 2005-305 du 8 décembre 2005 tel que modifié par la délibération n° 2010-369 du 14 octobre 2010 relatif aux finalités du traitement est supprimé et est désormais rédigé comme suit :

« 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 au sein de l'organisme dans les domaines suivants :

1. Financier, comptable, bancaire et de la lutte contre la corruption ;
2. Pratiques anticoncurrentielles ;
3. Lutte contre les discriminations et le harcèlement au travail ;
4. Santé, hygiène et sécurité au travail ;
5. Protection de l'environnement,

et ce dès lors que la mise en œuvre de ces traitements répond à une obligation légale ou à un intérêt légitime dans ces domaines. »

Art. 2. – L'article 2 de la délibération n° 2005-305 du 8 décembre 2005 relatif au traitement de l'identité de l'émetteur d'alerte est supprimé.

Le nouvel article 2 de l'AU-004 relatif aux alertes anonymes est rédigé comme suit :

« 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 :

1. La gravité des faits mentionnés est établie et les éléments factuels sont suffisamment détaillés ;
2. 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. »

Art. 3. – L'article 12 inséré par la délibération n° 2010-369 du 14 octobre 2010 est supprimé.

La présente délibération sera publiée au *Journal officiel* de la République française.

Pour la présidente :
Le vice-président délégué,
E. DE GIVRY