

RECOMMANDATION N° 01 / 2006 du 29 novembre 2006

N. Réf. : SA2 / SE / 2006 / 059

OBJET : Recommandation relative à la compatibilité des systèmes d'alerte interne professionnelle avec la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel.

La Commission de la protection de la vie privée ;

Vu la loi du 8 décembre 1992 *relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel* (ci-après la LVP), en particulier l'article 30 ;

Vu le nombre croissant de questions adressées à la Commission visant à savoir à quelles conditions un règlement de système d'alerte interne professionnelle est compatible avec la LVP ;

Vu le rapport de Madame N. LEPOIVRE et de Monsieur F. ROBBEN ;

Emet, le 29 novembre 2006, la recommandation suivante :

Définition

Les systèmes d'alerte professionnelle (whistleblowing) sont des dispositions permettant à des individus de signaler un comportement d'un membre de leur organisation contraire, selon eux, à une législation ou à une réglementation ou aux règles primordiales établies par leur organisation.

Contexte

Par la présente recommandation, la Commission estime nécessaire de préciser sa position sur les systèmes d'alerte interne professionnelle en général étant donné que de tels systèmes sont de plus en plus fréquents dans tous les pays de l'Union européenne et donc également en Belgique¹. Différentes questions et une plainte officielle ont d'ailleurs déjà été adressées à la Commission quant à la légitimité de tels systèmes à la lumière de la LVP.

En outre, des avocats, dont les clients veulent d'une part honorer leurs obligations découlant de la loi américaine "Sarbanes-Oxley" (ci-après dénommée la "SOX"), laquelle a notamment des incidences pour les entreprises étrangères cotées à la bourse de New York et pour les filiales étrangères d'entreprises américaines, et d'autre part être en règle avec les prescriptions en matière de protection des données contenues dans 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 et dans la LVP, interrogent également la Commission.

Les principes fondamentaux que la Commission estime devoir retenir ci-après pour considérer que de tels systèmes d'alerte sont conformes à la LVP peuvent dès lors servir de fil conducteur pour les organisations qui envisagent de mettre en œuvre ces systèmes d'alerte ou, au besoin, d'adapter ceux déjà existants.

Exercice d'équilibre

La mise en œuvre d'un système d'alerte implique un exercice d'équilibre dans lequel les intérêts légitimes de tous les protagonistes (l'organisation, son personnel, le dénonciateur, la personne mise en cause et les tiers éventuels) doivent être conciliés.

Un système d'alerte poursuit en effet plusieurs finalités, tant pour l'organisation que pour le personnel.

L'intérêt de l'organisation se traduit par le besoin de faire respecter la réglementation et ses règles internes et par le souci de sauvegarder son image grâce à un contrôle interne efficace.

Pour le personnel, il est important d'éviter la détérioration de l'ambiance au sein de l'organisation. Le fait d'éviter les tensions dues à une "culture de dénonciation" et un traitement correct du dénonciateur et de la personne mise en cause peuvent notamment y contribuer.

Un encadrement adéquat est donc nécessaire afin d'une part, d'éviter les alertes injustifiées et d'autre part, de traiter correctement les alertes justifiées.

¹ Apparemment aussi dans le secteur public. Voir par exemple l'article 12bis du décret "médiation" du 7 juillet 1998 modifié par le décret du 7 mai 2004 : *"Tout membre du personnel attaché à une autorité administrative telle que visée à l'article 3, peut dénoncer par écrit ou oralement auprès du service de médiation flamand, des négligences, abus ou délits tels que visés à l'article 3, § 2, et aux conditions y décrites."*

Pour être complet, la Commission indique que l'organe consultatif européen indépendant sur la protection des données et de la vie privée (appelé ci-après le Groupe 29) a émis le 1^{er} février 2006 un avis *relatif à l'application des règles de l'UE en matière de protection des données aux mécanismes internes de dénonciation des dysfonctionnement dans les domaines de la comptabilité, des contrôles comptables internes, de l'audit, de la lutte contre la corruption et la criminalité bancaire et financière*.

Applicabilité de la LVP

La mise en place d'un système d'alerte engendre une situation dans laquelle la LVP trouve à s'appliquer dans la mesure où des données à caractère personnel seraient traitées de façon automatisée ou même si elles étaient contenues ou appelées à figurer dans un fichier (article 3 de la LVP). La Commission estime donc que dans quasi la totalité des cas, l'utilisation d'un système d'alerte impliquera automatiquement un traitement de données à caractère personnel au sens de la LVP. Le traitement de données à caractère personnel dans le cadre d'un tel système d'alerte doit dès lors être conforme aux prescriptions de la LVP.

Dispositions applicables de la LVP

La Commission estime que les données à caractère personnelles doivent être traitées en respectant les dispositions suivantes de la LVP:

- admissibilité, loyauté, licéité et finalité (articles 4 et 5 de la LVP) ;
- proportionnalité (article 4, § 1, 3° de la LVP) ;
- exactitude et précision (article 4, § 1, 4° de la LVP) ;
- transparence (article 9 de la LVP) ;
- sécurité (article 16 de la LVP) ;
- pour toutes les personnes dont sont détenues des données à caractère personnel dans le cadre du système d'alerte (et notamment le dénonciateur et la personne mise en cause) : droits d'accès, de rectification et de suppression des données à caractère personnel les concernant (articles 10 et 12 de la LVP) ;
- obligation de déclaration (articles 17 et 19 de la LVP).

Admissibilité, loyauté, licéité et finalité

Admissibilité

En ce qui concerne l'admissibilité, la Commission trouve à l'article 5 de la LVP deux bases légales possibles permettant à une organisation de justifier son système d'alerte à savoir :

- 1° l'existence d'une obligation légale ou réglementaire lui imposant de traiter des données à caractère personnel via un système d'alerte (article 5, c) de la LVP) ;
- 2° en l'absence d'une telle obligation légale, un intérêt légitime dans son chef à condition que ne prévalent pas l'intérêt ou les droits et libertés fondamentaux de la personne mise en cause (article 5, f) de la LVP).

Dans la mesure où les données fournies et traitées sont des données à caractère personnel au sens de l'article 8 de la LVP, en l'espèce des données à caractère personnel concernant des suspicions relatives à des infractions, l'article 5 de la LVP ne suffit pas pour permettre à l'organisation de traiter les données visées. En principe, il y a même une interdiction de traitement (article 8, § 1 de la LVP), laquelle peut toutefois être levée, si l'organisation peut invoquer un fondement légal ou réglementaire pour le traitement exceptionnel de ces données tel que précisé à

l'article 8, § 2 de la LVP. Tel sera le cas si le traitement est nécessaire à la réalisation de finalités établies par ou en vertu d'une loi, d'un décret ou d'une ordonnance (article 8, § 2, b) de la LVP) ou si le traitement est nécessaire pour la gestion des propres contentieux de l'organisation (article 8, § 2, c) de la LVP) et moyennant le respect de conditions supplémentaires telles que prévues à l'article 25 de l'arrêté royal du 13 février 2001 *portant exécution de la LVP*².

Pour pouvoir parler d'une obligation légale au sens de l'article 5, c) de la LVP en respect de laquelle une organisation est tenue de traiter des données à caractère personnel via un système d'alerte, il doit s'agir d'une disposition légale du droit belge. Une obligation légale étrangère ne peut pas entrer ici en ligne de compte. La Commission partage à cet égard le point de vue du Groupe 29³ et des Commissions de protection de la vie privée française⁴ et néerlandaise⁵.

A titre exemplatif, la section 301 (4) de la SOX qui prévoit que les collaborateurs d'une entreprise doivent pouvoir exprimer leur préoccupation auprès du comité d'audit concernant des problèmes comptables ou relatifs à l'audit tout en étant assurés de bénéficier de garanties en matière de confidentialité et d'anonymat, constitue certes une obligation légale étrangère.

Pour apprécier l'intérêt légitime de l'organisation au sens de l'article 5, f) de la LVP, il convient de prendre en considération la gravité des faits reprochés ainsi que les aspects de proportionnalité et de subsidiarité.

En cas d'obligation imposée par une législation étrangère, cette législation ne pourra constituer un intérêt pour une organisation que dans la mesure où le système d'alerte est instauré pour assurer le respect des dispositions obligatoires de cette réglementation. Par exemple, la SOX n'exige, semble-t-il, des signalements que dans les domaines comptable ou d'audit.

Sans entrer dans la controverse qui existe concernant l'applicabilité extraterritoriale de la législation américaine précitée, la Commission comprend que pour les entreprises belges cotées à la bourse de New York, les obligations imposées par la législation SOX doivent être respectées afin d'éviter divers problèmes et sanctions.

² - les catégories de personnes, ayant accès aux données à caractère personnel, doivent être désignées par le responsable du traitement ou, le cas échéant, par le sous-traitant, avec une description précise de leur fonction par rapport au traitement des données visées ;

- la liste des catégories des personnes ainsi désignées doit être tenue à la disposition de la Commission par le responsable du traitement ou, le cas échéant, par le sous-traitant ;

- il doit veiller à ce que les personnes désignées soient tenues, par une obligation légale ou statutaire, ou par une disposition contractuelle équivalente, au respect du caractère confidentiel des données visées ;

- lorsque l'information, due en vertu de l'article 9 de la LVP, est communiquée à la personne concernée ou lors de la déclaration visée à l'article 17, § 1^{er}, de la LVP, le responsable du traitement doit mentionner la base légale ou réglementaire autorisant le traitement de données à caractère personnel visées aux articles 6 à 8 de la LVP.

³ Le Groupe 29 a déclaré à cet égard que : "Une obligation imposée par une loi ou un règlement étrangers qui exigeraient l'établissement de systèmes de signalement ne saurait être qualifiée d'obligation légale légitimant le traitement des données dans l'UE. Toute autre interprétation permettrait à des législations étrangères de contourner les règles fixées par l'UE avec la directive 95/46/CE".

⁴ Document d'orientation adopté par la Commission nationale de l'informatique et des libertés le 10 novembre 2005 pour la mise en œuvre de dispositifs d'alerte professionnelle conformes à la loi du 6 janvier 1978 modifiée en août 2004, relative à l'informatique, aux fichiers et aux libertés.

⁵ Avis du 16 janvier 2006 relatif à la demande d'autorisation ex. art. 77, alinéa 2 de la loi néerlandaise WBP du College Bescherming Persoonsgegevens.

Les conséquences pour une organisation qui ne satisferait pas à cette obligation légale étrangère doivent donc également être considérées pour retenir une éventuelle application de l'article 5, f) de la LVP.

Loyauté, licéité et finalité

Le champ d'application et la finalité du système d'alerte, donc le type de signalements qui peuvent être effectués par le dénonciateur via le système d'alerte interne, ainsi que les limites de la portée de ce système doivent être décrits avec précision.

L'organisation doit également veiller à une description précise de la procédure d'introduction et de traitement des signalements (qui, quoi, où, quand, comment, ...).

Le système doit décrire clairement quelles sont les conséquences des alertes justifiées et injustifiées.

Le responsable du traitement, auprès duquel les droits d'accès, de rectification et de suppression des données à caractère personnel peuvent être exercés, tant par le dénonciateur que par la personne mise en cause, doit être explicitement désigné.

Le système d'alerte ne peut pas prévoir, pour les membres du personnel, l'obligation de dénoncer. L'utilisation du système d'alerte doit donc avoir un caractère facultatif.

Le dénonciateur doit avoir un motif raisonnable pour suspecter la situation problématique qu'il signale. De simples rumeurs ne sont donc pas suffisantes.

Les signalements et les informations mentionnées doivent être suffisamment précis. L'acceptation de signalements trop vagues pourrait en effet alimenter une "culture de dénonciation", ce qui doit bien entendu être évité.

Etant donné ce qui précède, la Commission est favorable à une interdiction de principe des signalements anonymes. La question de savoir si le rapport, dans le cadre de règlements de systèmes d'alerte, doit se faire de manière anonyme ou ouverte (c'est-à-dire avec la connaissance de l'identité du dénonciateur par « le gestionnaire de plaintes ») a fait l'objet d'une attention particulière dans l'avis du Groupe 29 dont il est question ci-avant. La Commission souscrit à l'argumentation développée en la matière par le Groupe 29 qui autorise de manière très restrictive et en l'entourant d'exigences particulières le traitement de signalements anonymes et promeut au contraire le signalement avec l'identification du dénonciateur.

Lors du traitement du signalement, le système d'alerte doit prévoir une interdiction de communiquer l'identité du dénonciateur ou des éléments qui peuvent permettre son identification sans son accord.

Ce n'est que lorsque le signalement est traité et que les incriminations sont soit justifiées, soit manifestement fausses que le résultat peut être communiqué à l'organisation.

Le signalement doit être recueilli et traité par une personne spécialement désignée au sein de l'organisation pour instruire les plaintes. Cette personne (appelé dans cette recommandation « le gestionnaire de plaintes ») doit être tenue au secret professionnel lors du traitement de l'alerte, même à l'égard des dirigeants (sauf si des mesures conservatoires immédiates s'imposaient), des autres membres du personnel, des organisations syndicales et des tiers.

«Le gestionnaire de plaintes» doit pouvoir opérer avec suffisamment d'indépendance par rapport à l'organisation. Le système d'alerte doit prévoir des garanties quant à l'absence d'incompatibilités avec cette fonction. Ce gestionnaire doit agir en ayant une responsabilité précise et dès lors pouvoir être interpellé, par exemple en cas de violation de son devoir de confidentialité à l'égard du dénonciateur, de la personne mise en cause ou des tiers lors du traitement du signalement.

«Le gestionnaire de plaintes» doit être protégé contre les pressions qu'il pourrait subir de la hiérarchie ou des syndicats, d'autant plus que la personne mise en cause peut elle-même faire partie de la hiérarchie ou des syndicats.

«Le gestionnaire de plainte» doit traiter l'alerte avec un maximum de discrétion.

Le traitement du signalement par «le gestionnaire de plaintes» dans le cadre de la procédure d'alerte prend fin en cas de violation intentionnelle de cette confidentialité par le dénonciateur lui-même.

Le système d'alerte doit prévoir une protection du dénonciateur et de la personne mise en cause à l'encontre d'éventuelles fautes du «gestionnaire de plainte».

Proportionnalité

Une limitation du champ d'application

En principe, les procédures de contrôle normales d'ordre hiérarchique, comptable ou autre, exercées par des personnes qui représentent la direction de l'organisation et dont la tâche est justement de détecter et de traiter les dysfonctionnements dans l'entreprise, doivent suffire à dissiper leurs préoccupations relatives aux comportements de transgression de la norme par le personnel.

Le système d'alerte interne peut uniquement servir de canal spécifique et subsidiaire par lequel tous ou certains membres du personnel désignés dans le système d'alerte peuvent faire état d'irrégularités graves au sein de l'entreprise.

La Commission souligne le caractère strictement complémentaire du système d'alerte. Il ne peut s'agir que de signalements concernant des problèmes qui ne peuvent manifestement pas être traités par la voie hiérarchique normale et pour lesquels il n'existe pas de procédure ou d'organe spécifique réglementé légalement (pour ce dernier aspect, on peut par exemple penser à la problématique du harcèlement au travail ou du harcèlement sexuel).

Il ne peut s'agir que de signalements relatifs à des faits suffisamment graves (infractions à la réglementation applicable à l'organisation concernée ou à des règles d'entreprise internes écrites (notamment dans les domaines financier, comptable ou pénal). Il doit donc s'agir de dysfonctionnements sérieux –(sans être nécessairement des infractions) – mais néanmoins des faits ou des situations suffisamment graves qu'il faut dénoncer dans l'intérêt général ou dans celui d'une bonne gouvernance de l'organisation et pour lesquels le dénonciateur estime ne pas ou plus pouvoir suivre la voie hiérarchique normale, (par exemple lorsque le signalement précédent n'a pas été traité correctement par la hiérarchie, ou lorsque celle-ci est elle-même impliquée dans le problème signalé par le dénonciateur, ...).

Seules les personnes qui font partie de l'organisation peuvent dénoncer ou faire l'objet de signalements dans les domaines où le système d'alerte s'applique.

«Le gestionnaire de plaintes»

«Le gestionnaire de plaintes» doit veiller à ce que les données à caractère personnel :

- soient adéquates, pertinentes et non excessives pour le traitement du signalement ;
- restent limitées à la désignation de faits et ne contiennent en principe pas de jugement de valeur. Des appréciations subjectives doivent donc en règle générale être rejetées ;
- soient mentionnées expressément en tant que telles si elles concernent des faits non prouvés ;
- soient conservées pour une durée n'excédant pas celle nécessaire au traitement du signalement, y compris les éventuelles procédures judiciaires ou disciplinaires à l'encontre de

la personne mise en cause (en cas de signalement justifié) ou à l'encontre du dénonciateur en cas de signalements injustifiés ou d'accusations calomnieuses.

Exactitude et précision

«Le gestionnaire de plaintes» a la responsabilité de veiller, éventuellement avec l'aide d'instances internes ou externes suffisamment indépendantes (pour faire procéder à certaines vérifications), à ce que les données à caractère personnel destinées au traitement des signalements soient exactes et précises.

Transparence

Niveau collectif

L'organisation qui souhaite mettre en place un système d'alerte doit en informer son personnel en respectant les législations sur le droit collectif du travail (en informant, s'il échet, le conseil d'entreprise, le comité pour la protection et la prévention du travail, la délégation syndicale ou les comités de négociation ou de concertation).

Niveau individuel

Tous les collaborateurs de l'organisation susceptibles d'être impliqués dans le système d'alerte doivent être informés :

- du champ d'application et des finalités du système d'alerte ;
- de la procédure d'introduction et de traitement des signalements ;
- des conséquences de signalements justifiés et injustifiés ;
- de la manière dont les droits d'accès, de rectification et de suppression peuvent être exercés ainsi que de l'instance auprès de laquelle ces droits peuvent être exercés ;
- des tiers à qui des données à caractère personnel concernant le dénonciateur et la personne mise en cause peuvent être transmises dans le cadre du traitement du signalement, par exemple le service d'audit interne si «le gestionnaire de plaintes» doit faire vérifier certaines choses.

Il importe de signaler au dénonciateur l'obligation de confidentialité lors de l'introduction du signalement et au cours du traitement de celui-ci.

La personne mise en cause doit être informée le plus rapidement possible par «le gestionnaire de plaintes» de l'existence d'un signalement et des faits qui lui sont reprochés afin de lui permettre d'exécuter ses droits prévus par le chapitre III de la LVP.

L'information de la personne mise en cause peut être reportée dans des circonstances exceptionnelles (par exemple, en cas de risque de destruction de preuves).

Sécurité

Le système d'alerte doit prévoir des garanties afin que les données à caractère personnel traitées dans le cadre de signalements ne soient pas traitées à d'autres fins. Il doit donc s'agir d'un traitement distinct des autres traitements.

Il doit prévoir des garanties d'intégrité, d'authenticité, de disponibilité et de confidentialité des données à caractère personnel.

Il doit assurer que des données à caractère personnel ne peuvent pas être détruites de façon illégale lors du traitement du signalement.

Il doit organiser des possibilités d'audit permettant de connaître la manière dont les données à caractère personnel ont été traitées (contrôle visant à savoir qui a fait quoi, avec quelles données à caractère personnel et à quel moment).

La garantie de l'anonymat du dénonciateur et des éventuelles parties intervenantes est également un élément important au niveau de la sécurité.

Les données à caractère personnel ne peuvent pas être exportées vers des pays tiers hors Union Européenne, sauf dans le respect des dispositions de la LVP concernant le transfert des données (art. 21-22 de la LVP).

Un transfert de données à la maison mère dans un pays tiers hors de l'Union européenne ne sera justifié que s'il s'agit de situations problématiques particulièrement graves pour lesquelles il est devenu évident que le traitement du signalement ne peut pas ou plus se faire correctement exclusivement au niveau de l'organisation européenne ou qu'elles ont des répercussions au-delà de la société établie en Belgique ou dans l'U.E..

Droits de la personne mise en cause, du dénonciateur, des tiers

Tous les intervenants dans le système d'alerte ont tous les droits prévus au chapitre III de la LVP sur leurs données à caractère personnel.

Ils ont donc un droit de rectification de leurs données à caractère personnelles qui seraient incorrectes ainsi que le droit de faire supprimer ces mêmes données qui seraient incomplètes ou non pertinentes, dont le traitement est interdit, ou qui sont conservées après le traitement du signalement.

Ils n'ont aucun droit à accéder aux données à caractère personnelles d'autrui à moins que ces derniers n'y aient expressément donné leur accord.

La personne mise en cause ne peut donc pas accéder à l'identité du dénonciateur ou à celle de tiers (ou à des éléments qui permettraient leur identification), sauf s'ils ont donné leur accord, ou en cas de signalement injustifié ou d'accusations calomnieuses du dénonciateur ou de faux témoignage d'un tiers.

Le dénonciateur n'a pas non plus le droit d'accéder aux données à caractère personnelles de la personne mise en cause ni des tiers. Cette interdiction d'accès pourrait toutefois être levée lorsque, après enquête, il apparaît que la personne mise en cause a suspecté à tort le dénonciateur (en affirmant par exemple que le dénonciateur était lui-même impliqué dans les pratiques abusives qu'il a dénoncées) ou si des tiers ont agi de mauvaise foi (par exemple des personnes interrogées faisant de faux témoignages).

Le dénonciateur a le droit de savoir ce qu'il advient de son signalement ainsi que les suites qui y sont données.

Déclaration

Préalablement à sa mise en œuvre, une déclaration de tout système d'alerte qui prévoit un traitement de données à caractère personnel de manière automatisée, est obligatoire auprès de la Commission (application de l'article 17 de la LVP).

Si, dans le cadre du système d'alerte, les données à caractère personnel sont reprises dans un fichier manuel ou sont destinées à y être reprises, aucune déclaration n'est en principe requise, sauf si la Commission le demandait (article 19 de la LVP). En l'espèce, cette exigence semble être rencontrée, vu le caractère particulier des données à caractère personnelles (parfois des données visées par l'article 8 de la LVP, données relatives à des suspicions d'infractions) qui seront traitées.

Et ce d'autant plus qu'il s'agira d'une collecte de données à caractère personnel visant à porter un jugement sur les personnes concernées.

Rapports d'évaluation du système d'alerte

La Commission ne s'oppose pas à ce que des rapports d'évaluation du système d'alerte soient effectués. Ces rapports ne peuvent toutefois pas être communiqués sous une forme permettant l'identification des personnes concernées.

La Commission souhaite faire remarquer à cet égard que la suppression de données d'identification à l'égard des personnes concernées ne peut pas toujours empêcher qu'elles soient de nouveau identifiées. En d'autres termes, le risque que leur identité soit quand même révélée de manière indirecte ne peut pas être entièrement exclu. Plus la nature de la plainte, les problèmes organisationnels et/ou structurels constatés et les recommandations formulées seront décrits en détails dans le rapport, plus le risque de violation de l'anonymat requis sera grand, ce qui doit être évité.

PAR CES MOTIFS,

La Commission estime que les systèmes d'alerte sont seulement compatibles avec la LVP s'ils respectent, à tout le moins, les principes fondamentaux mentionnés ci-dessus. Ces principes peuvent donc servir de fil conducteur pour les organisations qui envisagent de mettre en œuvre de tels systèmes ou, au besoin, d'adapter de tels systèmes déjà existants.

L' administrateur,

Le vice-président,

(sé) Jo BARET

(sé) Willem DEBEUCKELAERE