LE CONTRÔLEUR EUROPÉEN
DE LA PROTECTION DES DONNÉES

GIOVANNI BUTTARELLI
CONTRÔLEUR ADJOINT

M. Alain LEFÈBVRE
Délégué à la protection des données de
l'Agence européenne des produits
chimiques
Annankatu 18
P.O. Box 400
FI-00121 HELSINKI
Finlande

Bruxelles, le 25 octobre 2011
GB/UK/mch/ D(2011)1867 **C 2011-0012**

Objet: Dossier n° 2011-12 relatif à la notification d'un contrôle préalable sur le système de vidéosurveillance à l'Agence européenne des produits chimiques (ECHA)

Monsieur,

Nous avons examiné les documents que vous avez communiqués au Contrôleur européen de la protection des données (CEPD) le 21 décembre 2010 concernant la notification d'un contrôle préalable sur les traitements liés au système de vidéosurveillance de l'Agence européenne des produits chimiques (ECHA), conformément à l'article 27 du règlement (CE) n° 45/2001 (le règlement).

Le CEPD a adopté des lignes directrices en matière de vidéosurveillance[1] (ci-après, les «lignes directrices») en mars 2010, en demandant aux organes et institutions de l'UE de mettre leurs pratiques actuelles en conformité avec ces lignes directrices pour le 1er janvier 2011. Dans le présent dossier, sur la base de la notification du 21 décembre 2010, le CEPD ne mettra en exergue que les pratiques de l'ECHA qui ne semblent pas conformes aux principes du règlement et aux lignes directrices et limitera son analyse juridique à ces pratiques. Il est clair que toutes les recommandations pertinentes formulées dans les lignes directrices s'appliquent aux traitements mis en place dans le cadre du système de vidéosurveillance à l'Agence européenne des produits chimiques.

[1] http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Guidelines/10-03-17_Video-surveillance_Guidelines_FR.pdf

La section 4.3 des lignes directrices décrit les situations dans lesquelles le CEPD considère que la notification d'un contrôle préalable prévue à l'article 27 du règlement est nécessaire pour aider l'institution concernée à instaurer des garanties supplémentaires de protection des données lorsque ses activités vont au-delà des traitements courants pour lesquels les lignes directrices fournissent déjà des garanties suffisantes. Les situations évoquées à la section 4.3 des lignes directrices portent notamment sur:

- la vidéosurveillance envisagée à des fins d'enquête;
- le traitement de catégories spéciales de données et
- l'utilisation de vidéosurveillance intelligente ou de haute technologie.

Comme la notification l'indique, les séquences produites par le système de vidéosurveillance à l'ECHA «peuvent, dans des cas exceptionnels, être également utilisées à des fins d'enquête (procédures disciplinaires)» et «les caméras installées dans la partie extérieure du bâtiment sont susceptibles d'enregistrer des images de manifestations passant devant les bâtiments de l'ECHA, ce qui peut ensuite donner lieu au traitement de catégories spéciales de données.» La section 4.2 de la politique de vidéosurveillance de l'ECHA indique en outre que «les caméras infrarouges peuvent être utilisées aux points d'entrée et de sortie extérieurs si d'autres mesures de sécurité sont inefficaces». La section 6.9 des lignes directrices énumère les dispositifs pouvant être qualifiés d'«outils de vidéosurveillance de haute technologie» ou de «systèmes de vidéosurveillance intelligents», ces derniers comprenant notamment les «caméras infrarouges ou quasi-infrarouges».

Les traitements à l'examen sont donc soumis à un contrôle préalable ex-post, conformément à l'article 27 du règlement.

Toutefois, ainsi que le CEPD l'a souligné lors de la publication des lignes directrices[2], ce n'est que dans des cas exceptionnels que le contrôle préalable est exhaustif et qu'il couvre *tous* les aspects d'un système de vidéosurveillance. Dans la plupart des cas, le CEPD n'examine *pas* de manière exhaustive toutes les pratiques de l'institution en matière de vidéosurveillance. Au lieu de cela, comme c'est le cas en l'occurrence, le CEPD concentre généralement ses recommandations sur les aspects de vidéosurveillance qui s'écartent des pratiques classiques et garanties standard exposées dans les lignes directrices ou qui viennent s'y ajouter.

1. Procédures

La procédure a été notifiée le 21 décembre 2010 en vue du contrôle préalable prévu à l'article 27 du règlement (CE) n° 45/2001. Elle a été suspendue par courrier électronique du 1er mars 2010 (D-420) au motif que la section 15.1 des lignes directrices prévoit que «à partir du 1er janvier 2011, et après avoir reçu les documents demandés, le CEPD établira un calendrier de traitement des notifications de contrôle préalable ex-post. En fonction du nombre et de la qualité des notifications de contrôle préalable ex-post reçues, de l'éventail de problèmes rencontrés et d'autres facteurs pertinents, le CEPD pourra émettre des avis individuels ou des avis communs portant sur plusieurs institutions et/ou problèmes.»

[2] Voir «Frequently asked questions on video-surveillance: prior checking» (Foire aux questions sur la vidéosurveillance: contrôle préalable), section 5, disponible à l'adresse suivante: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Guidelines/10-03-17_FAQ_videosurveillance_EN.pdf.

2. Vidéosurveillance envisagée à des fins d'enquête (procédures disciplinaires)

Faits: D'après la notification et la section 3.1 de la politique de vidéosurveillance de l'ECHA, les séquences vidéo «ne seront utilisées dans des procédures disciplinaires que dans des cas exceptionnels, lorsque les images filmées prouvent qu'un membre du personnel a manqué aux obligations qui lui incombent, notamment celles énoncées dans le statut des fonctionnaires et ses modalités d'application, le code de bonne conduite administrative de l'ECHA et les règles de sécurité de l'ECHA, ou lorsqu'une infraction pénale présumée a été filmée». L'analyse d'impact jointe à la notification indique à cet égard que «l'utilisation de séquences vidéo dans des procédures disciplinaires a évidemment une incidence sur la vie privée de la personne concernée, mais cette incidence ne semble pas disproportionnée au regard de la finalité étant donné que seules les séquences enregistrées «accidentellement» seront utilisées et que le système ne prendra jamais pour cible un individu donné. L'absence de surveillance cachée étaye également ce point de vue».

D'après la section 1 de la politique de vidéosurveillance de l'ECHA, le système de vidéosurveillance de l'ECHA a été mis en place à des fins typiques de sécurité. La section 5.8 des lignes directrices énonce que «lorsqu'un système est mis en place à des fins typiques de sécurité, les enregistrements vidéo peuvent servir à enquêter sur les incidents physiques de sécurité, par exemple l'accès non autorisé aux locaux ou à des pièces protégées, le vol, le vandalisme, un incendie ou l'agression physique d'une personne. […] En principe toutefois, les systèmes de vidéosurveillance ne doivent pas être installés ou conçus à des fins d'enquêtes internes dépassant le cadre des incidents de sécurité tels que ceux décrits ci-dessus».

Dans ce contexte, l'utilisation prévue des séquences lorsqu'«un membre du personnel a manqué aux obligations qui lui incombent, notamment celles énoncées dans le statut des fonctionnaires et ses modalités d'application, le code de bon comportement administratif de l'ECHA et les règles de sécurité de l'ECHA» est source d'inquiétudes quant à sa proportionnalité:

- La gravité d'une infraction au code de conduite d'une institution n'est généralement pas semblable à une infraction pénale ou aux incidents de sécurité physique visés à la section 5.8 des lignes directrices. La section 5.1.3 des lignes directrices indique explicitement que «lorsqu'un système de vidéosurveillance est installé à des fins de sécurité, et annoncé comme tel au personnel, les enregistrements ne peuvent pas être utilisés […] à des fins d'enquête ni comme preuves dans le cadre d'enquêtes internes ou de procédures disciplinaires, sauf dans le cas d'un incident de sécurité physique ou, dans des cas exceptionnels, de comportement criminel».

- La section 5.9 des lignes directrices précise en outre que «des objectifs tels que […] le respect des règlements des institutions […] ne justifient pas la vidéosurveillance d'employés dans le contexte du travail des institutions» et souligne que les mesures de contrôle exagérément intrusives peuvent causer un stress inutile aux employés et éroder leur confiance dans l'organisation.

Recommandations:

- En l'absence d'autres justifications spécifiques de l'utilisation de la vidéosurveillance à des fins d'enquête et de garanties procédurales faisant en sorte qu'une évaluation appropriée de la proportionnalité a lieu dans ces cas, les séquences vidéo ne peuvent être utilisées par l'ECHA dans le cadre de procédures disciplinaires lorsqu'un membre du personnel a manqué aux obligations qui lui incombent,

notamment celles énoncées dans le statut des fonctionnaires et ses modalités d'application, le code de bonne conduite administrative de l'ECHA et les règles de sécurité de l'ECHA.

- En l'absence d'autres justifications spécifiques de l'utilisation de la vidéosurveillance à des fins d'enquête et de garanties procédurales faisant en sorte qu'une évaluation appropriée de la proportionnalité a lieu dans ces cas, la section 3.1 de la politique de vidéosurveillance de l'ECHA doit être modifiée en conséquence de manière à limiter l'utilisation de séquences vidéo dans les procédures disciplinaires aux cas exceptionnels où les images enregistrées prouvent un incident de sécurité physique ou un comportement délictuel.

3. Traitement de catégories particulières de données (manifestations)

Faits: D'après la notification, les séquences vidéo peuvent même comprendre «dans certains cas, des données révélant des opinions politiques (si une manifestation passant devant les locaux de l'ECHA est enregistrée)».

L'analyse d'impact fournie indique à cet égard ceci: «…Étant donné que les locaux de l'Agence sont situés dans le centre-ville d'Helsinki, la capitale finlandaise, ... il est tout à fait possible qu'une manifestation passe devant le bâtiment et que des images des manifestants soient enregistrées accidentellement. Il peut même y avoir un besoin accru de vidéosurveillance pour garantir la sécurité des locaux, du personnel et des visiteurs pendant les manifestations. Même s'il existe à cet égard un risque évident pour la vie privée des manifestants, l'Agence n'enregistre que des images pour ses propres besoins de sécurité aux abords immédiats des points d'entrée et de sortie du bâtiment. La politique en matière de vidéosurveillance garantit en outre qu'aucune séquence de manifestations pacifiques n'est transférée à une tierce partie».

La section 4.7 de la politique de vidéosurveillance de l'ECHA prévoit en effet que «les séquences de catégories spéciales de données (par exemple, de manifestations) ne sont pas transférées en l'absence d'indice clair d'infraction pénale». Elle ne précise toutefois pas dans quelles circonstances un indice d'infraction pénale est jugé «clair» en ce sens et ne fait pas référence aux garanties procédurales concernées.

Si le CEPD se réjouit du fait que, comme il l'avait recommandé précédemment[3], une analyse d'impact se focalisant sur cette question particulière ait été prévue au cas où des manifestations se tiennent régulièrement aux abords du bâtiment et où les manifestants sont susceptibles d'entrer dans le champ de vision des caméras, l'analyse d'impact prévue semble ne pas satisfaire aux normes applicables en vertu des lignes directrices:

- Comme on peut le lire à la section 5.6 des lignes directrices, «même si une institution arrive à la conclusion qu'il existe un besoin réel d'utiliser la vidéosurveillance et qu'il n'existe pas d'autre méthode moins intrusive, elle ne doit avoir recours à cette technologie que si les effets négatifs de la vidéosurveillance sont compensés par ses avantages… il faut trouver un équilibre difficile entre les intérêts légitimes et les droits fondamentaux des personnes concernées et les bénéfices escomptés de la vidéosurveillance». Alors que la politique de vidéosurveillance de l'ECHA prévoit qu'aucune séquence de manifestations pacifiques n'est *transférée* à une tierce partie, l'*enregistrement* de séquences vidéo constitue déjà un traitement de données devant

[3] http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Guidelines/10-07-14_Videosurveilllance_followup_EN.pdf

être justifié. La section 7.1.4 des lignes directrices recommande d'envisager notamment la surveillance en direct lorsque celle-ci est nécessaire pour réduire au minimum l'impact sur le respect de la vie privée et d'autres droits fondamentaux et intérêts légitimes des personnes passant dans le champ de vision des caméras.

- D'après la section 5.7 des lignes directrices, les institutions doivent justifier, de façon vérifiable, l'existence et l'ampleur des risques de sécurité allégués (dangers spécifiques, taux de criminalité, etc.). La simple «perception» d'un risque, la spéculation et les anecdotes ne suffisent pas à démontrer la nécessité de la vidéosurveillance. Cette analyse des risques doit être documentée par écrit et doit identifier et évaluer tous les risques existants et les institutions doivent démontrer les risques de sécurité présents sur le site surveillé en décrivant les incidents de sécurité qui s'y sont produits par le passé ou qui risquent de s'y produire à l'avenir.

- La section 5.7 des lignes directrices prévoit également qu'avant d'opter pour la vidéosurveillance, il est important d'envisager soigneusement toutes les alternatives moins intrusives. Il peut s'agir, par exemple, de contrôles effectués par le personnel de sécurité, d'une mise à niveau des systèmes d'alarme, de systèmes de contrôle d'accès, de l'installation de barrières, portes et fenêtres blindées et renforcées ou encore d'un meilleur éclairage. La vidéosurveillance ne doit être utilisée que si l'insuffisance de ces solutions a été démontrée.

Recommandations:

- À la lumière de la section 5.7 des lignes directrices, l'ECHA doit justifier, de façon vérifiable, l'existence et l'ampleur des risques de sécurité allégués (dangers spécifiques, taux de criminalité, etc., au lieu de faire référence en des termes vagues au «besoin accru de vidéosurveillance pour garantir la sécurité des locaux, du personnel et des visiteurs pendant les manifestations») et démontrer:
  - le type de risques pour la sécurité dans la zone surveillée en indiquant le genre d'incidents de sécurité qui y ont eu lieu par le passé ou qui sont susceptibles de s'y produire à l'avenir et en étayant cette analyse des risques par écrit;
  - que toutes les alternatives moins intrusives (par exemple, les contrôles effectués par le personnel de sécurité, la mise à niveau des systèmes d'alarme, les systèmes de contrôle des accès, l'installation de barrières, portes et fenêtres blindées et renforcées et un meilleur éclairage) n'apportent pas une réponse suffisante aux problèmes de sécurité identifiés.

- À la lumière de la section 5.6 des lignes directrices, l'ECHA doit prouver qu'elle a très soigneusement mis en balance les intérêts légitimes et les droits fondamentaux des personnes surveillées avec les avantages pouvant résulter de la surveillance.

- Au cas où l'ECHA devrait être en mesure de prouver l'existence et l'ampleur des risques de sécurité allégués et le juste équilibre entre les bienfaits de la vidéosurveillance et les intérêts légitimes et droits fondamentaux des personnes surveillées, le CEPD lui recommande, si aucun incident de sécurité n'a été détecté, d'effacer les enregistrements de toute manifestation pacifique au plus tard dans un délai de deux heures après la fin de la manifestation.

- Bien que la section 4.7 de la politique de vidéosurveillance de l'ECHA fasse généralement référence aux transferts aux autorités nationales, le CEPD souhaite rappeler les principes suivants énoncés à la section 10.4 des lignes directrices:
  - Si la police, un tribunal ou d'autres autorités nationales demandent la divulgation d'enregistrements, l'institution doit insister pour recevoir une demande écrite respectant les obligations de forme et de contenu imposées par la législation nationale en vigueur. L'institution ne doit divulguer ces enregistrements que dans les cas où une autre institution installée dans ce pays, dans des circonstances similaires, aurait été obligée ou au moins autorisée à les divulguer.
  - Chaque fois que possible et indépendamment des obligations imposées au niveau national, l'institution doit demander un mandat judiciaire, une demande écrite signée par un officier de police suffisamment gradé ou une demande formelle similaire. Cette demande devrait aussi spécifier, le plus précisément possible, la raison pour laquelle la séquence de vidéosurveillance est nécessaire ainsi que l'endroit, la date et l'heure de la séquence demandée.
  - Les demandes générales en vue d'une exploration des données (*data mining*) doivent être rejetées.

  L'ECHA doit veiller à ce que les garanties précitées s'appliquent aux transferts de séquences vidéo aux autorités nationales. Le CEPD note à cet égard que, d'après la section 4.7 de la politique de vidéosurveillance de l'ECHA, «le responsable de la sécurité consulte le délégué à la protection des données de l'Agence sur toutes les demandes de transfert». Étant donné les implications que le transfert des séquences de manifestation a pour les intérêts légitimes et droits fondamentaux des personnes surveillées, le CEPD invite l'ECHA à garantir dans la procédure que la consultation du DPD est obligatoire dans ces cas.

4. Utilisation de vidéosurveillance intelligente ou de haute technologie (caméras infrarouges)

Bien que la notification ne fasse pas explicitement référence à la question, la section 4.2 de la politique de vidéosurveillance de l'ECHA qui lui est jointe indique que «les caméras infrarouges peuvent être utilisées aux points d'entrée et de sortie extérieurs si d'autres mesures de sécurité sont inefficaces». La section 6.9 des lignes directrices énumère les dispositifs pouvant être qualifiés d'«outils de vidéosurveillance de haute technologie» ou de «systèmes de vidéosurveillance intelligents» et fait explicitement référence aux caméras infrarouges dans ce contexte.

Comme indiqué à la section 6.9 des lignes directrices, l'introduction d'«outils de vidéosurveillance de haute technologie» ou de «systèmes de vidéosurveillance intelligents» n'est autorisée que moyennant une analyse d'impact. L'analyse d'impact produite ne fait cependant pas allusion à cette question.

Recommandation:
Afin de permettre au CEPD d'évaluer la licéité de la technique utilisée et d'imposer au besoin des garanties particulières de protection des données, l'ECHA doit lui fournir une analyse d'impact couvrant l'utilisation prévue de caméras infrarouges aux points d'entrée et de sortie extérieurs si d'autres mesures de sécurité sont inefficaces.

5. Rappels concernant d'autres aspects de la politique de vidéosurveillance de l'ECHA

a) Surveillance ad hoc

La section 4.7 de la politique de vidéosurveillance de l'ECHA prévoit qu'à condition qu'une vidéosurveillance ad hoc constitue «une contre-mesure efficace», elle peut être mise en œuvre si le responsable de la sécurité le décide, par exemple en raison de la présence d'hôtes de marque ou d'une augmentation temporaire du risque de sécurité, ou parce que d'autres systèmes physiques ne fonctionnent pas. Cette section ne contient toutefois aucune précision ou ligne directrice. Conformément à la section 3.5 des lignes directrices, l'institution qui envisage d'utiliser la vidéosurveillance sur une base ad hoc (par exemple lors de l'organisation d'événements importants ou dans le cadre d'enquêtes internes) doit également dresser des plans à l'avance. Dans ce cas, le cadre et les politiques nécessaires pour la protection des données doivent être mis en place suffisamment longtemps avant la vidéosurveillance elle-même. La politique de vidéosurveillance de l'ECHA doit être complétée par un cadre aidant le responsable de la sécurité à prendre sa décision et décrivant dans les grandes lignes les mesures à appliquer.

b) Nombre de caméras mentionné dans la politique

D'après la section 6.2 des lignes directrices, le nombre de caméras doit être mentionné dans la politique de vidéosurveillance. La politique de vidéosurveillance de l'ECHA ne mentionne pas cette information et doit donc être complétée en ce sens.

c) Période de conservation

D'après la section 4.6 de la politique de vidéosurveillance de l'ECHA, la période normale de conservation est de 28 jours calendaires (quatre semaines), soit une durée plus longue que celle recommandée à la section 7.1 des lignes directrices, «en raison des risques accrus posés par l'emplacement de l'Agence et la valeur des informations traitées dans ses locaux, et parce que les locaux ont de nombreux points d'entrée et de sortie répartis dans plusieurs bâtiments séparés mais reliés entre eux. Ce dernier aspect peut avoir pour effet que les incidents de sécurité ne sont découverts qu'après un certain laps de temps…».

Le CEPD souhaite souligner que, comme l'illustre l'exemple donné à la section 7.1.3 des lignes directrices[4], le fait qu'une institution est située dans un centre-ville animé ne peut en soi justifier une dérogation à la période de conservation normale recommandée dans les lignes directrices. Cela n'exclut pas, bien entendu, qu'une institution prouve, de façon vérifiable, l'existence et l'ampleur des risques de sécurité allégués[5], notamment un taux de criminalité élevé dans ses environs, qui peut contribuer entre autres choses à justifier l'instauration d'une période de conservation plus longue.

Comme le CEPD l'a précisé précédemment[6], si les institutions ne fournissent pas de justification suffisante et de garanties adéquates, elles doivent réduire la période de conservation à sept jours ou moins, conformément aux recommandations des lignes directrices. L'ECHA doit dès lors prouver, de façon vérifiable, l'existence et l'ampleur des risques de sécurité allégués, comme l'exige la section 5.7 des lignes directrices.

---

[4] «L'agence B est installée au cœur d'un centre-ville animé, à proximité d'une gare, avec une circulation piétonne importante sur le trottoir au pied de ses bâtiments».

[5] Voir la section 5.7 des lignes directrices.

[6] http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Guidelines/10-07-14_Videosurveilllance_followup_EN.pdf

d) Élimination des supports devenus inutilisables

Conformément à la section 7.1.1 des lignes directrices, la politique de vidéosurveillance de l'ECHA doit également prévoir ce qu'il y a lieu de faire lorsque le support est devenu inutilisable afin de garantir qu'il est supprimé en toute sécurité ou de telle manière que les données qu'il contient encore soient supprimées de façon permanente et irréversible.

e) Registre des enregistrements conservés au-delà de la période de conservation

D'après la section 7.2 des lignes directrices, l'ECHA doit tenir un registre des enregistrements conservés au-delà de la période de conservation.

f) Formation

L'ECHA est invitée à confirmer que la formation évoquée à la section 4.13 de sa politique de vidéosurveillance («…sera offerte…») a bien eu lieu.

g) Avis affiché sur place et version publique de la politique de vidéosurveillance de l'ECHA

La section 5.1.2 des lignes directrices prévoit que l'objectif du système doit être communiqué au public sous une forme sommaire à l'endroit concerné, et sous une forme plus détaillée, par exemple, via une version publique en ligne de la politique de vidéosurveillance de l'institution.

L'avis affiché sur place mentionné à la section 4.11 de la politique de vidéosurveillance de l'ECHA ne satisfait pas aux exigences de contenu visées à la section 11.2 des lignes directrices. L'ECHA doit revoir l'avis de manière à ce qu'il:

- identifie le «responsable du traitement» (le nom de l'institution est généralement suffisant);
- spécifie la finalité de la surveillance («pour votre sécurité» est généralement suffisant);
- indique clairement si les images sont enregistrées;
- fournisse des informations de contact et un lien vers la politique de vidéosurveillance disponible en ligne;
- indique clairement que la surveillance s'étend à des zones situées en dehors du bâtiment (voir ci-dessus). Dans un tel cas, un avis indiquant simplement que *le bâtiment* fait l'objet d'une vidéosurveillance prête à confusion.

Étant donné que seule la version «interne» de la politique de vidéosurveillance de l'ECHA a été fournie, l'ECHA est invitée à communiquer au CEPD la «version abrégée» mise à la disposition des visiteurs à la réception du bâtiment et visée à la section 4.11 de ladite politique.

h) Annexes à la politique de vidéosurveillance

À la lumière du bordereau d'annexes à la politique de vidéosurveillance figurant à la page 63 des lignes directrices, l'ECHA est invitée à fournir au CEPD les documents suivants:

- un plan d'emplacement des caméras;
- les spécifications techniques des caméras et de l'ensemble du système de vidéosurveillance (matériel et logiciel compris);
- le contrat conclu avec l'entreprise de sécurité externe;
- des copies des accords de confidentialité (voir la section 8.3 des lignes directrices);
- le registre de conservation et de transferts (voir les sections 10.5 et 7.2 des lignes directrices);
- une politique de sécurité spécifique au traitement («politique de sécurité en matière de vidéosurveillance»).

6. Conclusions

Le CEPD invite l'ECHA à adopter des mesures spécifiques et concrètes pour mettre en œuvre les recommandations précitées concernant le système de vidéosurveillance.

Pour ce qui est des rappels mentionnés dans la présente note, le CEPD souhaite être informé de la situation concernant le respect des lignes directrices et recevoir les informations demandées.

Afin de faciliter notre suivi, nous vous saurions gré de bien vouloir transmettre au CEPD, dans un délai de trois mois à compter de la date de la présente lettre, tous les documents pertinents prouvant que l'ensemble des recommandations et rappels ont été mis en œuvre.

Veuillez croire, Monsieur, à l'assurance de ma considération distinguée.

(**signé**)

Giovanni BUTTARELLI