Avis concernant une notification en vue d'un contrôle préalable reçue par le délégué à la protection des données de la Banque centrale européenne concernant la «*procédure relative aux accidents et aux maladies professionnelles*»

Bruxelles, le 20 février 2014 (dossier 2012-0792)

1. Procédure

Le 14 septembre 2012, le Contrôleur européen de la protection des données («le CEPD») a reçu une notification de contrôle préalable au sens de l'article 27, paragraphe 3, du règlement n° 45/2001 («le règlement») concernant la «procédure relative aux accidents et aux maladies professionnelles» du délégué à la protection des données («le DPD») de la Banque centrale européenne («la BCE»).

Depuis la réception de la notification, le CEPD a échangé plusieurs courriers avec le DPD en vue d'obtenir des informations complémentaires et des précisions concernant le traitement en cause.

Le projet d'avis a été soumis aux commentaires du DPD le 4 février 2014. Le CEPD a reçu une réponse le 12 février 2014.

2. Faits

Finalité et personnes concernées

La DG Ressources humaines, budget et organisation («la DG-H») est responsable de la gestion des procédures liées à la reconnaissance des accidents du travail et des maladies professionnelles afin de garantir le paiement des prestations et le remboursement des frais médicaux aux personnes concernées.

Les personnes concernées sont les membres du personnel de la BCE (et, lorsqu'ils sont impliqués, leurs conjoint, partenaire reconnu et/ou enfant à charge), les agents titulaires d'un contrat de travail de courte durée, les participants au programme pour jeunes diplômés de la BCE, les témoins potentiels et les tiers (blessés ou non) ayant un lien avec un accident.

Base juridique

La base juridique du traitement se compose des dispositions suivantes:

- articles 7,10, 16, 19, 28, 31, 32, 33 et 34 des conditions d'emploi de la BCE;
- annexe IV aux conditions d'emploi de la BCE et
- articles 12, 27, 28, 29 et 30 des conditions d'emploi des titulaires de contrats de travail de courte durée de la BCE.

Procédure et données traitées

La collecte d'informations initiale est réalisée manuellement et sur la base de documents papier, comme les rapports de médecins. Ces informations sont numérisées dans une base de données informatique.

En cas d'accident du travail ou de maladie professionnelle, les personnes concernées doivent soumettre le formulaire de notification d'accident ou la demande de reconnaissance d'une maladie professionnelle aux personnes responsables de la fonction «Santé et sécurité» au sein de la DG-H.

Elles doivent également soumettre un certificat médical et toutes autres pièces justificatives au médecin-conseil de la BCE dans une enveloppe scellée. Le directeur général de la DG-H ou son adjoint, sur la base de l'avis médical d'expert d'un ou de plusieurs médecins (médecins du service médical de la BCE ou médecins externes), adopte la décision définitive concernant la reconnaissance d'un accident du travail, de la nature professionnelle d'une maladie et la détermination du degré d'invalidité permanente après consolidation des blessures.

Le médecin-conseil de la BCE et les médecins externes sont des experts médicaux indépendants et sont soumis à la législation de l'État membre de l'UE dans lequel ils travaillent. À titre d'exemple, en Allemagne, ils sont liés par un régime contractuel et légal qui leur impose des obligations strictes de confidentialité et de secret professionnel en application de l'article 203, paragraphe 1, point 1, du code pénal allemand (StGB). Ils sont désignés officiellement par le directeur général de la DG-H ou par son adjoint [et/ou par le président de l'Association médicale de l'état de Hessen dans le cas de recours (Hessische Landesärztekammer)] qui délivrent une «*lettre de désignation d'un expert médical (ou d'experts médicaux)*». La BCE et les médecins externes (experts médicaux) sont liés par un contrat tacite conclu par l'effet de la «*lettre de désignation d'un expert médical (ou d'experts médicaux)*» qui couvre les aspects liés à la protection des données (qui renvoient à l'article 10 du règlement).

Aucune communication directe n'intervient entre les médecins externes désignés et la DG-H au-delà des éléments strictement administratifs de la procédure, à savoir la soumission de documents, le paiement des frais, etc. Les médecins/experts externes communiquent leurs conclusions médicales au médecin-conseil de la BCE. Sur la base de ces conclusions médicales, le médecin-conseil de la BCE prépare des informations non confidentielles à l'attention des responsables de la fonction «Santé et sécurité» au sein de la DG-H.

Dans le cas d'une procédure de recours, la commission médicale (article 6, paragraphe 6, des règles applicables au personnel de la BCE), à l'issue de ses délibérations, adopte son avis sous la forme d'un rapport médical. La commission médicale fournit également un résumé comportant des informations non confidentielles exposées dans ce rapport aux responsables de la section «Santé et sécurité» de la DG-H.

En cas d'accident sans lien avec l'activité professionnelle, les personnes blessées doivent soumettre une demande d'indemnisation à un **assureur externe**, **par l'intermédiaire d'un administrateur externe**. Les tâches de l'assureur se limitent à régler les litiges et à assumer les risques. L'administrateur externe fournit à la DG-H des informations non confidentielles concernant les accidents subis par les personnes concernées à des fins statistiques, de gestion des contrats et d'achat, à savoir: 1) l'identité des membres du personnel qui ont signalé l'accident, 2) la date de l'accident, 3) la catégorie d'accident, 4) le point de savoir si l'accident a entraîné une incapacité permanente et, dans l'affirmative, le niveau d'indemnisation, et 5) le cas échéant, le refus de reconnaissance d'un accident et les motifs de ce refus. La BCE a conclu un contrat avec l'assureur externe et l'administrateur externe, qui sont tous deux soumis à l'une des législations des États membres de l'UE et le contrat comporte des dispositions relatives à la protection des données, à la confidentialité et à la sécurité.

En outre, la BCE a conclu un contrat avec **un autre administrateur externe** pour le remboursement des frais médicaux dans le cadre des prestations médicales et du régime relatif aux soins dentaires de la BCE. L'administrateur externe reçoit directement des membres du personnel un formulaire de demande de remboursement des frais médicaux, accompagné des factures, et procède au remboursement des personnes concernées. Le contrat est soumis à l'une des législations des États membres de l'UE et comporte des dispositions relatives à la protection des données, à la confidentialité et à la sécurité.

Autres données traitées

Outre les données de nature administrative et liées à l'accident de la personne concernée, le formulaire de notification d'accident doit comporter ou être accompagné des éléments suivants: le rapport de police, s'il est disponible, les noms et adresses du ou des témoins et le nom, l'adresse et l'indication de la compagnie d'assurance de tout tiers impliqué dans un accident, qu'il ait ou non été blessé.

En outre, la demande de remboursement des frais médicaux doit comporter l'indication, entre autres éléments, du nom du conjoint, du partenaire reconnu et/ou de l'enfant à charge si cette ou ces personnes ont été également blessées lors d'un accident avec le membre du personnel.

Tous les responsables de la section «Santé et sécurité» de la DG-H ainsi que les personnes travaillant au centre médical de la BCE ont signé des déclarations de confidentialité aux termes desquelles ils sont liés par des obligations de secret professionnel. Ces déclarations de confidentialité renvoient également aux dispositions du règlement.

Destinataires

Conformément à la procédure susmentionnée, les destinataires des données traitées sont les suivants:

Destinataires externes

- le médecin-conseil de la BCE qui reçoit tous les certificats médicaux, l'historique des examens médicaux des personnes concernées et le formulaire de demande de reconnaissance d'une maladie professionnelle;
- les médecins externes reçoivent les mêmes informations que le médecin-conseil de la BCE;

- l’assureur externe du régime d’assurance-accident, qui reçoit, par l’intermédiaire de l’administrateur externe, un formulaire de notification d’accident ou de maladie professionnelle, les certificats médicaux justificatifs après la visite médicale, les certificats médicaux délivrés dans le cadre de la procédure relative aux accidents du travail et aux maladies professionnelles pertinents concernant la stabilisation de l’état de santé et des certificats médicaux aux fins de la détermination du degré d’invalidité permanente;
- l’administrateur externe des prestations médicales et du régime relatif aux soins dentaires de la BCE, qui reçoit un formulaire de demande de remboursement des frais médicaux, accompagné de factures, des membres du personnel.

Droits d’accès et de rectification

Les personnes concernées peuvent avoir accès aux données médicales les concernant qui sont détenues par le médecin-conseil de la BCE et en réaliser des copies. Elles peuvent également avoir accès aux données à caractère personnel les concernant qui sont détenues par la DG-H.

Elles disposent également du droit de rectification et du droit de verser à leur dossier médical les contre-avis d’un autre médecin ou une décision de justice pertinente à cet égard.

Droit à l’information

La déclaration de confidentialité concernant les données relatives à la santé renvoie à certaines des informations énumérées aux articles 11 et 12 du règlement.

Elle est insérée dans tous les formulaires (formulaire de notification d’accident du travail, formulaire de notification d’accident sans lien avec l’activité professionnelle, demande de reconnaissance d’une maladie professionnelle) qui sont accessibles au public sur le site intranet.

Politique de conservation

Toutes les données administratives et financières sont conservées dans les dossiers personnels pendant une durée maximale de 10 ans à compter de la cessation de l’emploi du membre du personnel au sein de la BCE ou du dernier versement de pension.

Les certificats médicaux et les documents relatifs à la santé soumis dans le cadre d’accidents et de maladies professionnelles sont conservés pendant une durée maximale de cinq ans à compter de la date de leur soumission.

Les **dossiers médicaux papier** sont conservés pendant une durée de 30 ans à compter de la clôture du dossier. Les données figurant dans le **logiciel médical** seront conservées pendant une durée de 10 ans à compter de la clôture du dossier.

Comme l’a expliqué le DPD de la BCE, à l’heure actuelle, les règles relatives à la conservation de la BCE n’abordent pas spécifiquement le dossier médical papier mais, plus généralement, les données à caractère personnel. En ce qui concerne la période de conservation du dossier médical, la BCE a lancé la procédure de modification des règles applicables au personnel de la BCE concernant la période de conservation des dossiers médicaux. La période de conservation des données médicales conservées sous forme papier sera alignée sur celle des données médicales conservées sous forme électronique.

Conformément à la notification, il n'est envisagé aucun traitement ultérieur à des fins historiques, statistiques ou scientifiques. Cependant, comme il est indiqué ci-dessus en page 2 et sur la base des informations complémentaires communiquées par le responsable du traitement, l'administrateur externe fournit à la DG-H des données anonymes agrégées annuellement concernant les dossiers d'assurance et les prestations d'assurance à des fins statistiques, de gestion des contrats et d'achat.

Conservation et mesures de sécurité

Les dossiers médicaux sont conservés dans des armoires verrouillées (meubles résistant au feu) au service médical de la BCE. Les données médicales seront également conservées sous forme électronique dans le logiciel médical et comprendront tous les rapports médicaux supplémentaires, les rapports du médecin-conseil de la BCE et la décision définitive adoptée par le directeur général de la DG-H ou son adjoint. Seuls le médecin-conseil et les infirmiers ont accès au dossier médical de la personne concernée et au logiciel médical. Les données électroniques sont cryptées dans la base de données et les utilisateurs comme les modifications doivent être approuvés et autorisés par le centre médical de la BCE.

Le formulaire de notification d'accident, les notes relatives aux congés pour maladie délivrées par le médecin-conseil de la BCE ou par un autre médecin, la demande de reconnaissance d'une maladie professionnelle et les décisions définitives adoptées par le directeur général de la DG-H sont conservés séparément dans une partie spécifique du dossier personnel. Seuls les responsables de la fonction «Santé et sécurité» de la DG-H se voient accorder un accès à cette partie. Les dossiers personnels sont conservés dans des armoires sécurisées.

3. Aspects juridiques

3.1 Contrôle préalable

Application du règlement: le traitement de données examiné constitue un traitement de données à caractère personnel [«*toute information concernant une personne physique identifiée ou identifiable*», article 2, point a), du règlement]. Le traitement des données est effectué par une institution de l'Union européenne, la BCE, dans l'exercice d'activités qui relèvent du champ d'application du droit européen.[1] Le traitement des données est à la fois manuel - les données étant incluses ou destinées à être incluses dans un système de classement (rapports médicaux, dossiers médicaux), et automatique (les informations sont enregistrées dans une base de données informatique). Le règlement est donc applicable en l'espèce.

Motifs de contrôle préalable: l'article 27, paragraphe 1, du règlement soumet à un contrôle préalable effectué par le CEPD tous «*les traitements susceptibles de présenter des risques particuliers au regard des droits et libertés des personnes concernées du fait de leur nature, de leur portée ou de leurs finalités*». L'article 27, paragraphe 2, du règlement contient une liste des traitements susceptibles de présenter de tels risques. Conformément à l'article 27, paragraphe 2, point a), du règlement, «*les traitements de données relatives à la santé*» sont soumis au contrôle préalable du CEPD. Il en va ainsi en l'espèce, puisque les données relèvent des données relatives à la santé.

[1] Les notions d'«institutions et organes de la Communauté» et de « droit communautaire » ne peuvent plus être utilisées depuis l'entrée en vigueur du traité de Lisbonne le 1er décembre 2009. Dès lors, l'article 3 du règlement n° 45/2001 doit être lu à la lumière du traité de Lisbonne.

Notification et date d'échéance pour l'avis du CEPD: la notification du DPD a été reçue le 14 septembre 2012. Depuis la date de réception, le CEPD a échangé plusieurs courriers avec le DPD en vue de l'obtention d'informations complémentaires et de précisions concernant le traitement en cause. Le présent dossier ayant un caractère ex post, le délai de deux mois imparti au CEPD pour rendre son avis ne s'applique pas; ce dossier a été traité dans les meilleurs délais.

3.2 Licéité du traitement

Les données ne peuvent être traitées que pour l'un des motifs prévus par l'article 5 du règlement.

Des cinq motifs énumérés à l'article 5, le traitement à l'examen satisfait aux conditions prévues à l'article 5, point a), du règlement, à savoir que les données peuvent être traitées si le traitement est «*nécessaire à l'exécution d'une mission effectuée dans l'intérêt public sur la base des traités instituant les Communautés européennes* [...]».

En l'espèce, **la base juridique** du traitement figure dans les dispositions juridiques des conditions d'emploi de la BCE, telles qu'indiquées dans l'exposé des faits.

La nécessité du traitement est également citée au considérant 27 du règlement, qui précise que «*le traitement de données à caractère personnel effectué pour l' exécution de missions d' intérêt public par les institutions et organes communautaires comprend le traitement de données à caractère personnel nécessaires pour la gestion et le fonctionnement de ces institutions et organes*». Le traitement de données à caractère personnel en cause est nécessaire aux fins de la gestion du paiement des prestations et du remboursement des frais médicaux liés à des accidents du travail et à des maladies professionnelles aux personnes concernées. Dès lors, ce traitement permet d'assurer la bonne gestion des ressources humaines et le fonctionnement de la BCE.

3.3 Traitement de catégories particulières de données

L'article 10, paragraphe 1, du règlement prévoit que le traitement de données à caractère personnel relatives à la santé est interdit, sauf s'il est justifié par les motifs énoncés à l'article 10, paragraphes 2 et 3, du règlement.

L'article 10, paragraphe 2, point b), s'applique en l'espèce: «*Le paragraphe 1* (interdiction du traitement de données relatives à la santé) *ne s'applique pas lorsque* […] *le traitement est nécessaire afin de respecter les obligations et les droits spécifiques du responsable du traitement en matière de droit du travail, dans la mesure où il est autorisé par les traités instituant les Communautés européennes ou d'autres actes législatifs adoptés sur la base de ces traités* […]». Le traitement examiné est jugé nécessaire afin de respecter les obligations et les droits particuliers de la BCE en tant qu'employeur, en application du droit du travail. La BCE effectue donc ce traitement conformément aux dispositions de ses conditions d'emploi sur la base de l'article 10, paragraphe 2, point b), du règlement.

En outre, conformément à la notification, tous les responsables de la DG-H ainsi que les personnes travaillant au centre médical de la BCE sont liés par des obligations de secret professionnel au moyen de déclarations de confidentialité. L'article 10, paragraphe 3, du règlement est donc respecté.

3.4 Qualité des données

Adéquation, pertinence et proportionnalité: conformément à l'article 4, paragraphe 1, point c), du règlement, les données à caractère personnel doivent être «*adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et pour lesquelles elles sont traitées ultérieurement*». Il y a dès lors lieu de vérifier que les données collectées sont pertinentes au regard des finalités pour lesquelles elles sont traitées.

Les données décrites dans le présent avis semblent satisfaire à ces conditions au regard des finalités du traitement présenté ci-dessus.

Exactitude: l'article 4, paragraphe 1, point d), du règlement dispose que les données doivent être «*exactes et, si nécessaire, mises à jour*». En application de cet article, «*toutes les mesures raisonnables doivent être prises pour que les données inexactes ou incomplètes, au regard des finalités pour lesquelles elles sont collectées ou pour lesquelles elles sont traitées ultérieurement, soient effacées ou rectifiées*».

En l'espèce, les procédures en place permettent de conclure que le système prévoit une garantie raisonnable de qualité des données. Cependant, le CEPD relève que la période de conservation des données médicales figurant dans des dossiers papier est différente de celle des données médicales détenues sous forme électronique. Il pourrait exister un risque que, du fait de l'existence de périodes de conservation différentes des mêmes données présentées sous des formes différentes, l'exactitude des données médicales des personnes concernées ne soit pas pleinement garantie. Le CEPD recommande donc à la BCE de prendre toutes les mesures raisonnables pour assurer le respect du principe d'exactitude prévu à l'article 4, paragraphe 1, point d), du règlement (voir le développement concernant la période de conservation, point 3.5).

En ce qui concerne les droits d'accès et de rectification, la personne concernée semble en disposer, afin de veiller à ce que les données à caractère personnel la concernant et se rapportant à des accidents et à des maladies professionnelles soient aussi complètes que possible. Ces droits constituent le deuxième moyen de garantir que les données relatives à la personne concernée sont correctes et à jour (voir le développement concernant le droit d'accès, point 3.7).

Loyauté et licéité: l'article 4, paragraphe 1, point a), du règlement prévoit que les données à caractère personnel doivent être traitées «*loyalement et licitement*». La question de la licéité a déjà été analysée au point 3.2 du présent avis. Concernant la loyauté, elle est liée aux informations qui doivent être communiquées à la personne concernée (voir le développement concernant le droit à l'information, point 3.8).

3.5. Conservation des données

En vertu de l'article 4, paragraphe 1, point e), du règlement, les données à caractère personnel doivent être «*conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont collectées ou pour lesquelles elles sont traitées ultérieurement*».

Le CEPD considère que les périodes de conservation des données administratives et financières et des certificats médicaux liés au traitement en cause sont raisonnables et nécessaires à la réalisation des finalités pour lesquelles ils sont collectés ou pour lesquelles ils sont traités ultérieurement à la lumière de l'article 4, paragraphe 1, point e), du règlement.

En outre, le CEPD se félicite de l'initiative prise par la BCE de modification des règles applicables à son personnel concernant la période de conservation des dossiers médicaux et d'harmonisation de la période de conservation des données médicales sous forme papier et de celle des données médicales sous forme électronique. Le CEPD invite la BCE à prendre en considération les Lignes directrices du CEPD concernant le traitement des données relatives à la santé sur le lieu de travail[2], dans lesquelles il a recommandé l'application pour les dossiers médicaux sous forme papier et/ou électronique d'une période de conservation maximale de 30 ans à compter de la date à laquelle le dernier document médical a été inséré dans le dossier. En outre, le CEPD a souligné qu'il convient d'examiner la nature des documents médicaux, à la lumière de leur finalité et des règles applicables, afin de déterminer la période de conservation adaptée et nécessaire pour chaque type de document. Le CEPD recommande à la BCE d'adopter une période de conservation des dossiers médicaux à la lumière des Lignes directrices.

Enfin, le CEPD relève que ni la notification, ni la déclaration de confidentialité ne comporte d'indication claire de toutes les périodes de conservation décrites dans l'exposé des faits du présent avis. Le CEPD recommande à la BCE de mettre à jour les deux documents en conséquence.

En ce qui concerne la question des données anonymes agrégées, le CEPD relève que les informations figurant dans la notification sont inexactes, puisqu'il y est mentionné qu'il n'est envisagé aucun traitement ultérieur à des fins statistiques. Le CEPD recommande donc à la BCE d'indiquer dans la notification que l'administrateur externe fournit à la DG-H des données anonymes agrégées annuellement concernant les dossiers d'assurance et les prestations d'assurance à des fins statistiques, de gestion des contrats et d'achat.

3.6 Transfert de données

Les articles 7, 8 et 9 du règlement prévoient des obligations qui s'appliquent lorsque les responsables du traitement transfèrent des données à caractère personnel à des tiers. Les règles diffèrent selon que le transfert est effectué i) entre institutions ou organes de l'UE ou en leur sein (article 7), ou ii) à des destinataires relevant de la législation nationale adoptée en application de la directive 95/46/CE (article 8), ou iii) à des destinataires autres que les institutions et organes de l'UE et ne relevant pas de la directive 95/46/CE (article 9).

Transferts externes

La BCE a conclu des contrats avec son médecin-conseil, d'autres médecins externes, un assureur externe et un administrateur externe. Conformément à leurs contrats, ces personnes sont toutes soumises à l'une des législations des États membres de l'UE de transposition de la directive 95/46/CE. Ceci signifie que l'article 8 du règlement est applicable. Le CEPD considère que le transfert de données présenté dans l'exposé des faits est nécessaire à l'exécution par les destinataires précités de leur mission respective effectuée dans l'intérêt public, conformément à l'article 8, point a), du règlement.

[2] https://secure.edps.europa.eu/EDPSWEB/edps/Supervision/Guidelines.

3.7 Droits d'accès et de rectification

L'article 13 du règlement prévoit le droit d'accès aux données ainsi que les procédures applicables en la matière, à la demande de la personne concernée. L'article 14 du règlement prévoit le droit de rectification pour la personne concernée.

La notification et la note d'information renvoient à l'existence de ces deux droits et expliquent les modalités de l'exercice de ces droits par les personnes concernées. La BCE indique également la signification que revêt le droit de rectification dans le cadre du traitement de données relatives à la santé.

Cependant, le CEPD attire l'attention de la BCE sur l'article 20 du règlement, qui prévoit certaines limitations de ce droit, notamment lorsque ces dernières constituent une mesure nécessaire pour garantir la protection de la personne concernée ou des droits et libertés d'autrui. À titre d'exemple, les personnes concernées peuvent exercer leur droit d'accès direct à leur dossier médical dans les locaux du service médical de la BCE, en présence d'une personne désignée par celui-ci. Les rapports psychiatriques/psychologiques, en ce qui les concerne, peuvent être consultés par les personnes concernées par l'intermédiaire d'un médecin désigné par la personne concernée. En ce qui concerne les notes personnelles du médecin, les personnes concernées peuvent ne pas y avoir accès si, aux termes de l'article 20, paragraphe 1, point c) et sur la base d'un examen au cas par cas, cette limitation est nécessaire pour garantir la protection de la personne concernée ou des droits et libertés d'autrui.

Le CEPD recommande donc à la BCE d'expliquer, dans la note d'information, que l'article 20 du règlement peut s'appliquer de manière restrictive dans des cas exceptionnels. Le CEPD invite la BCE à examiner toute limitation potentielle de l'accès aux dossiers médicaux au cas par cas, conformément au principe de proportionnalité. L'article 20 du règlement ne doit pas aboutir à une interdiction totale d'accès aux notes personnelles des médecins figurant dans le dossier médical.

3.8 Information de la personne concernée

Les articles 11 et 12 du règlement concernent les informations à fournir aux personnes concernées afin d'assurer un traitement transparent des données à caractère personnel. En l'espèce, certaines données sont collectées directement auprès de la personne concernée et d'autres le sont auprès d'autres personnes (par exemple les médecins, les fonctionnaires de la DG-H, l'assureur, l'administrateur, des témoins potentiels ou des tiers blessés).

En l'espèce, la déclaration de confidentialité énonce la plupart des informations figurant aux articles 11 et 12 du règlement. Cependant, le CEPD recommande à la BCE de compléter la déclaration de confidentialité en y ajoutant les informations ci-après:

- périodes de conservation de tous les types de données à caractère personnel traitées, comme expliqué au point 3.5 de l'avis;
- précisions sur le droit d'accès, tel qu'évoqué au point 3.7 du présent avis.

En outre, le CEPD relève que dans les cas d'accident, la BCE pourrait procéder au traitement des données à caractère personnel de témoins potentiels et de tiers (blessés ou non) ayant un lien avec l'accident. La BCE, en qualité de responsable du traitement en cause, est donc soumise, en application du règlement, à une obligation d'information de ces personnes concernées, lorsque les données sont collectées auprès d'elles. Le CEPD recommande à la BCE de préparer une brève déclaration de confidentialité conforme à l'article 11 du règlement et d'ajouter ces catégories de personnes concernées dans la notification, en qualité de personnes concernées potentielles dans les cas de survenance d'un accident.[3]

3.9 Sous-traitance

L'article 23 du règlement prévoit que, lorsque le traitement est effectué pour le compte du responsable du traitement, celui-ci doit s'assurer que son sous-traitant peut apporter des garanties suffisantes au regard des mesures de sécurité technique et d'organisation pour le traitement des données à caractère personnel.

En l'espèce, tous les sous-traitants externes sont liés par des contrats conclus avec la BCE qui sont régis par la législation de l'UE de transposition de la directive 95/46/CE et qui comprennent notamment des dispositions concernant la protection des données, la confidentialité et la sécurité. En conséquence, la BCE se conforme aux exigences posées à l'article 23 du règlement.

3.10 Mesures de sécurité

Conformément à l'article 22 du règlement relatif à la sécurité du traitement, «*le responsable du traitement met en œuvre les mesures techniques et organisationnelles appropriées pour assurer un niveau de sécurité approprié au regard des risques présentés par le traitement et de la nature des données à caractère personnel à protéger*». Ces mesures de sécurité doivent notamment empêcher toute diffusion ou tout accès non autorisés, toute destruction accidentelle ou illicite, toute perte accidentelle ou toute altération, ainsi que toute autre forme de traitement illicite.

Après examen des mesures de sécurité décrites dans la notification, rien ne porte à croire que les mesures mises en œuvre par la BCE ne sont pas conformes à l'article 22 du règlement.

4. Conclusion

Rien ne porte à croire à une violation des dispositions du règlement, pour autant que les considérations suivantes soient pleinement prises en considération. En particulier, la BCE devrait:

- prendre toutes les mesures raisonnables pour assurer le respect du principe d'exactitude dans les dossiers médicaux, sous leurs formes papier et électronique, à savoir harmoniser la période de conservation des données médicales sous forme papier et celle des données médicales sous forme électronique;

- adopter la période de conservation des dossiers médicaux recommandée dans les Lignes directrices du CEPD;

[3] Voir l'avis du CEPD du 27 juin 2012 sur la notification du Conseil concernant la «Gestion du Bureau Véhicules de Service», dossier 2012-0157.

- indiquer dans la notification que l'administrateur externe fournit à la DG-H des données anonymes agrégées annuellement concernant les dossiers d'assurance et les prestations d'assurance à des fins statistiques, de gestion des contrats et d'achat;

- expliquer dans la notification et dans la déclaration de confidentialité que l'article 20 du règlement concernant le droit d'accès au dossier médical peut s'appliquer. La BCE devrait s'assurer que les limitations de l'accès aux dossiers médicaux sont examinées au cas par cas, conformément au principe de proportionnalité;

- inclure dans la déclaration de confidentialité les informations indiquées au point 3.8 du présent avis;

- préparer une brève déclaration de confidentialité pour les témoins potentiels et les tiers (blessés ou non) ayant un lien avec un accident et ajouter ces personnes en tant que catégorie supplémentaire de personnes concernées dans la notification.

Fait à Bruxelles, le 20 février 2014.

(signé)

Giovanni BUTTARELLI
Contrôleur européen adjoint de la protection des données