Avis sur la notification d'un contrôle préalable reçue du délégué à la protection des données de la Commission européenne concernant l'«Analyse de risque pour la prévention et la détection de la fraude dans la gestion du FSE et du FEDER» – ARACHNE

Bruxelles, le 17 février 2014 (2013-0340)

1. PROCÉDURE

Le 17 mai 2013, le contrôleur européen de la protection des données (**CEPD**) a reçu une notification de contrôle préalable concernant le traitement de données à caractère personnel «Analyse de risque pour la prévention et la détection de la fraude dans la gestion du FSE et du FEDER – ARACHNE» de la part du délégué à la protection des données (**DPD**) de la Commission européenne (**Commission**).

Des questions ont été soulevées le 4 juin 2013, auxquelles le DPD de la Commission a répondu le 26 juin 2013. Entre-temps, une réunion s'est tenue entre le CEPD et les services de la Commission le 7 juin 2013. De nouvelles questions ont été transmises le 27 juin 2013; les réponses respectives ont été reçues le 30 octobre 2013. Le 18 novembre 2013, le CEPD a envoyé le projet d'avis au DPD pour observations. Le CEPD a reçu une réponse le 26 novembre 2013, sur la base de laquelle le CEPD a demandé le même jour une notification modifiée, qu'il a reçue le 29 novembre 2013. Le CEPD a demandé la tenue d'une réunion le 9 décembre 2013; celle-ci a eu lieu le 9 janvier 2014 et a été suivie de la présentation de nouveaux documents le 17 janvier 2014. Le 24 janvier 2014, un projet d'avis révisé a été envoyé pour observations au DPD, lequel a confirmé le 13 février 2014 ne pas avoir de remarques.

2. FAITS

Le système ARACHNE fait partie de la stratégie de prévention et de détection de la fraude de la Commission dans le domaine des Fonds structurels [Fonds social européen (FSE) et Fonds européen de développement régional (FEDER)]. L'aide au développement structurel est mise en œuvre par le biais d'un système de «gestion partagée», c'est-à-dire que les États membres sont responsables de la mise en œuvre de l'aide, mais que la responsabilité financière finale reste celle de la Commission. La Direction H de la direction générale (DG) Emploi, affaires sociales et inclusion et la Direction J de la DG Développement régional de la Commission ont la responsabilité principale de valider les informations fournies par les autorités couvertes par le FSE et le FEDER[1], de réaliser des audits externes dans les États membres de l'Union

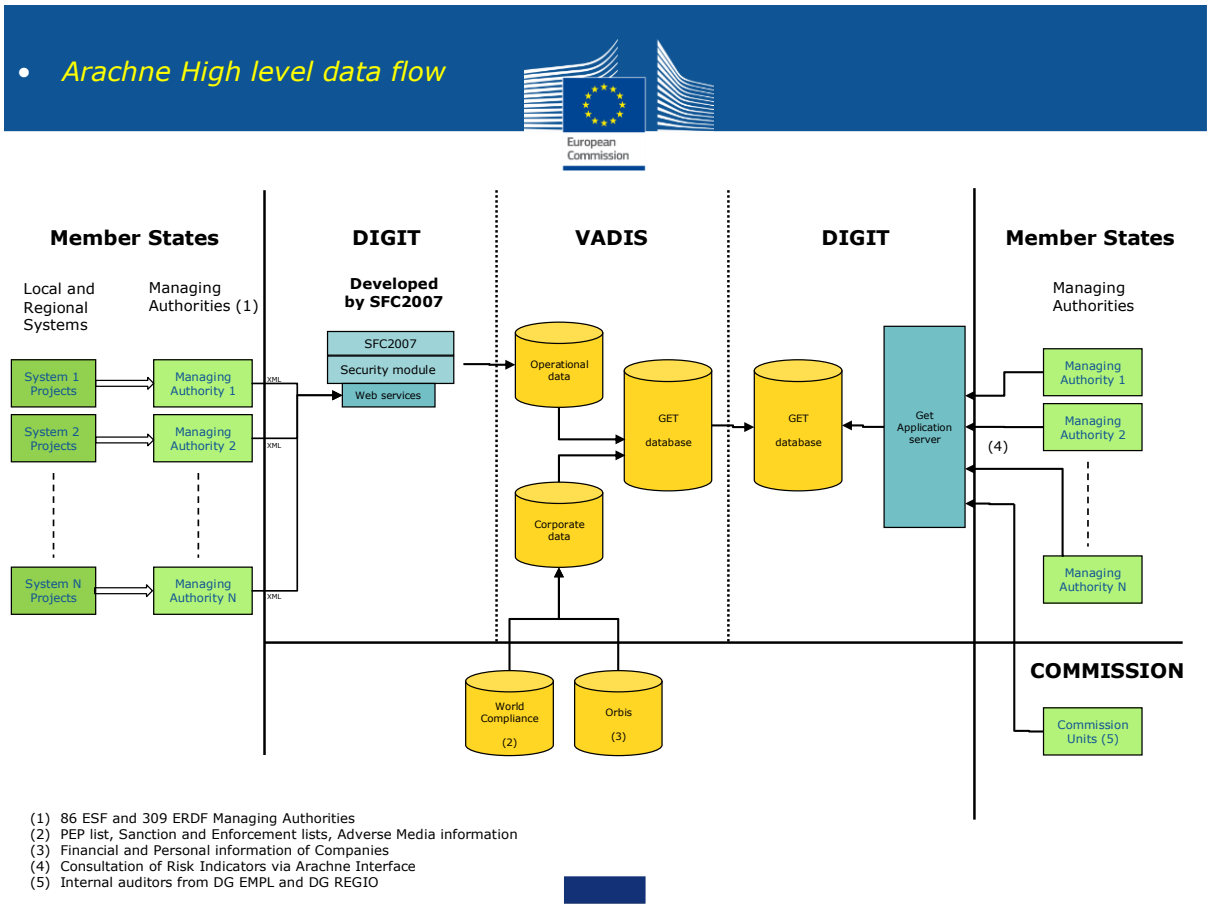
[1] Description du système de gestion et de contrôle, stratégie d'audit, rapport annuel de contrôle/avis annuel, rapports d'audit nationaux, synthèses annuelles.

Adresse postale: rue Wiertz 60 – B-1047 Bruxelles, Belgique
Bureaux: rue Montoyer 30
Courriel: edps@edps.europa.eu – Site Internet: www.edps.europa.eu
Tél.: +32 (0) 2-283 19 00 – Fax: +32 (0) 2-283 19 50

européenne, de publier des rapports et avis en temps opportun et de mettre à jour un tableau de notation des risques afin de permettre une gestion saine des Fonds.

La **finalité** du système ARACHNE est la détection de la fraude. Lors de la réunion du 9 janvier 2014, la Commission a explicitement confirmé qu'ARACHNE ne visait pas à évaluer le comportement individuel particulier de bénéficiaires de fonds et, en tant que tel, ne servait pas à exclure des bénéficiaires des Fonds. ARACHNE vient compléter une base de données existante des projets mis en œuvre dans le cadre des Fonds structurels («SFC») par des informations publiques afin d'identifier les projets les plus risqués, sur la base d'un ensemble d'indicateurs de risques. Lors de la réunion du 9 janvier 2014, il a été souligné que la notation du risque ne conduisait pas à une quelconque décision automatique contre des bénéficiaires. Les notations de risques sont utilisées pour aider les auditeurs à sélectionner/identifier de futurs candidats à un audit. ARACHNE, en tant que système, est basé sur l'intégration et la personnalisation d'un outil existant d'évaluation des risques, à savoir l'application GET de *VADIS Consulting SA/NV*, avec des données opérationnelles fournies par les autorités de gestion du FSE et du FEDER, afin de fournir des notations de risque permettant d'identifier les projets les plus risqués et les zones de risques spécifiques.

Dans une première étape de la **procédure**, l'infrastructure SFC2007 actuelle, une méthode de mise en place de services web transmettant des données opérationnelles des projets depuis les autorités de gestion du FSE et du FEDER des États membres vers la Commission, sera utilisée pour fournir des données opérationnelles à ARACHNE. Dans une deuxième étape, les données du projet seront complétées par des informations provenant de sources publiques. Dans une troisième étape, ARACHNE calculera des indicateurs de risque individuels (feuilles de notation des risques par projet) permettant une gestion saine des Fonds, y compris un contrôle continu de la finalité des projets d'audit.



Arachne High level data flow	Flux de données de haut niveau ARACHNE
Member States	États membres
Local and Regional Systems	Systèmes locaux et régionaux
Managing Authorities (1)	Autorités de gestion (1)
System 1 Projects	Projets système 1
System 2 Projects	Projets système 2
System N Projects	Projets système N
Managing Authority 1	Autorité de gestion 1
Managing Authority 2	Autorité de gestion 2
Managing Authority N	Autorité de gestion N
DIGIT	DIGIT
Developed by SFC2007	Développé par SFC2007
Security module	Module de sécurité
Web servicies	Services web
VADIS	VADIS
Operational data	Données opérationnelles
Get database	Base de données GET
Corporate data	Données d'entreprise
World Compliance (2)	Conformité monde (2)
Orbis (3)	Orbis (3)
DIGIT	DIGIT
Get application server (4)	Serveur applicatif GET (4)
COMMISSION	COMMISSION
Commission Units (5)	Unités de la Commission (5)
(1) 86 ESF and 309 ERDF Managing Authorities	(1) 86 autorités de gestion FSE et 309 FEDER
(2) PEP list, Sanction and Enforcement lists, Adverse Media information	(2) Liste PPE, listes de sanctions et d'application, informations Adverse Media
(3) Financial and Personal information of Companies	(3) Information financière et personnelle de sociétés
(4) Consultation of Risk Indicators via Arachne Interface	(4) Consultation d'indicateurs de risques via l'interface ARACHNE
(5) Internal auditors from DG EMPL and DG REGIO	(5) Auditeurs internes de la DG EMPL et la DG REGIO

Le **responsable du traitement** est la Commission, conjointement représentée par le directeur de la Direction H de la DG Emploi, affaires sociales et inclusion et la Direction J de la DG Développement régional. Selon les informations complémentaires reçues le 26 novembre 2013, la Commission ne collecte pas les données elle-même, mais celles-ci proviennent d'une base de données existante de projets mis en œuvre dans le cadre des Fonds structurels (SFC) ou du prestataire externe. *VADIS SA/NV*, en tant que sous-traitant d'*ATOS Belgium NV/SA*, effectue le traitement pour le compte de la Commission au sens de l'article 23 du règlement n° 45/2001 (désigné ci-après «le règlement»). *VADIS SA/NV*, en tant que **sous-traitant**, fournit la base de données GET en résultant à la Commission, qui héberge l'application GET pour les utilisateurs finaux. Comme cela a été confirmé lors de la réunion du 9 janvier 2014, *VADIS SA/NV* ne transfère pas de dossiers individuels et ne partage pas d'informations. Cette activité est régie par un contrat écrit remis le 17 janvier 2014, qui stipule en particulier que le sous-traitant agit sur les instructions du responsable du traitement et qui contient des clauses écrites énonçant les obligations prévues aux articles 21 et 22 du règlement qui incombent au sous-traitant.

Les **personnes concernées** sont des personnes physiques telles que les bénéficiaires, respectivement en qualité de gestionnaires et d'actionnaires publics de bénéficiaires qui sont des entités légales, recevant une aide du FSE et/ou du FEDER et, éventuellement, d'autres personnes entretenant des relations avec ceux-ci.

Selon la notification, la **base légale** du système ARACHNE comprend:

- articles 60, 61, 62, 69 et chapitre IV, sections 1 et 2, du règlement n° 1083/2006[2];
- articles 13, 14, 16, 19, 37 et section 7 du règlement n° 1828/2006[3];
- chapitre 2.2.3 de la Communication de la Commission sur la stratégie antifraude du 22 juin 2011[4];
- règlement n° 966/2012[5] à la lumière des articles 325 et 317 du traité sur le fonctionnement de l'Union européenne (TFUE).

Selon la notification, les **catégories de données traitées** sont les suivantes:
1) De la part des autorités de gestion du FSE et du FEDER (via l'infrastructure SFC2007):
- bénéficiaires: nom, adresse, numéro de TVA, rôle;
- personnel clé: nom, fonction/poste;
- sous-traitants: nom, adresse, numéro de TVA;
- experts clés pour les contrats de service: nom, date de naissance.

2) De sources de données publiques externes fournies par VADIS SA/NV:
a) Du prestataire commercial ORBIS (http://www.bvdinfo.com/Products/Company-Information/International/Orbis):

- informations exhaustives sur des sociétés;
- actionnaires / direction / personnel clé: nom, fonction/poste;

b) Du prestataire commercial WORLD COMPLIANCE:

- profils de personnes politiquement exposées (PPE), des membres de leur famille et de leurs proches associés;
- liste de sanctions, indiquant les individus et sociétés dont la note de risque est la plus élevée;
- liste d'application, contenant des informations reçues des autorités réglementaires et gouvernementales et le contenu d'alertes et d'actions contre des individus et des sociétés;
- lecture des journaux et magazines à la recherche d'informations liées/relatives aux risques (y compris les informations de grands journaux en ligne dans les États membres de l'Union européenne et dans des pays tiers).

Les **destinataires** sont les utilisateurs d'ARACHNE:

- les autorités de gestion et leurs organes intermédiaires dans les États membres, leurs autorités de certification et les autorités d'audit;
- la DG Emploi, affaires sociales et inclusion de la Commission et la Direction générale de la politique régionale (à chaque fois la seule unité des auditeurs), à l'exception de la Direction H de la DG Emploi, affaires sociales et inclusion et de la Direction J de la DG Développement régional;
- la Cour des comptes européenne et l'OLAF (à leur demande).

---

[2] Règlement (CE) n° 1083/2006 du Conseil du 11 juillet 2006 portant dispositions générales sur le Fonds européen de développement régional, le Fonds social européen et le Fonds de cohésion (JO L 210, 31.7.2006, p. 25).

[3] Règlement (CE) n° 1828/2006 de la Commission du 8 décembre 2006 établissant les modalités d'exécution du règlement (CE) n° 1083/2006 du Conseil portant dispositions générales sur le Fonds européen de développement régional, le Fonds social européen et le Fonds de cohésion, et du règlement (CE) n° 1080/2006 du Parlement européen et du Conseil relatif au Fonds européen de développement régional (JO L 371, 27.12.2006, p. 1).

[4] COM(2011) 376 final, disponible en anglais à l'adresse: http://ec.europa.eu/anti_fraud/documents/preventing-fraud-documents/ec_antifraud_strategy_en.pdf.

[5] Règlement n° 966/2012 du Parlement européen et du Conseil du 25 octobre 2012 relatif aux règles financières applicables au budget général de l'Union (JO L 298, 26.10.2012, p. 1).

L'autorité de gestion et ses organes intermédiaires sont seuls à disposer de droits de lecture et d'écriture. En cas de problèmes techniques, la DG Informatique de la Commission et *VADIS SA/NV* peuvent accéder aux informations.

Les personnes concernées sont **informées** du traitement par une déclaration relative à la protection des données publiée sur le site web du Fonds social européen qui, en plus des informations obligatoires visées aux articles 11 et 12 du règlement, explique comment fonctionne et intervient la gestion des risques dans le contexte d'ARACHNE et en précise la base légale.

S'agissant des **droits d'accès et de rectification** des personnes concernées, il convient de distinguer (a) les données détenues par les autorités de gestion et leurs organes intermédiaires dans les États membres gérant les fonds FSE et FEDER ou d'autres autorités nationales compétentes, qui sont soumises à la directive 95/46/CE, et (b) les données détenues par la Commission, qui sont soumises au règlement:

a) Comme indiqué dans la déclaration relative à la protection des données (notifiée une nouvelle fois le 29 novembre 2013), les personnes concernées peuvent exercer leurs droits d'accès et de rectification des données détenues sur l'entité légale qu'elles représentent ou de leurs propres données à caractère personnel en adressant une demande aux autorités de gestion et à leurs organes intermédiaires dans les États membres traitant les fonds FSE et FEDER ou à d'autres autorités nationales compétentes. En cas de modification des données de projet, les autorités des États membres peuvent immédiatement modifier les données dans la base de données des projets mis en œuvre dans le cadre des Fonds structurels (SFC). Les personnes concernées sont également informées du fait qu'elles peuvent aussi contacter leur autorité nationale chargée du contrôle de la protection des données à caractère personnel en cas de difficultés ou de questions liées au traitement de ces données. Selon la notification, «*les États membres procèdent conformément à ce qui est prévu par la directive 95/46/CE*»;

b) S'agissant des informations provenant de sources médiatiques externes, que la Commission ne collecte pas elle-même, mais traite, le CEPD comprend que la «*personne concernée doit demander à connaître la source de l'information si elle a besoin que ses droits soient conférés <u>au-delà</u> du système ARACHNE*» (mis en exergue par l'auteur). L'octroi de droits d'accès et de rectification dans le contexte du système ARACHNE ne va pas *au-delà* de ce système.

Selon la déclaration relative à la protection des données, pour la Commission, «*l'article 20, paragraphe 1, point b), du règlement 45/2001 s'applique. Le droit d'accès des personnes concernées conformément à l'article 13 sera apprécié au cas par cas et reporté au cas où il pourrait donner des opportunités à de potentiels fraudeurs de trouver des faiblesses dans le processus d'évaluation des risques et de les contourner. Un accès sera accordé une fois la décision prise de ne pas réaliser d'audit ou à la date de réalisation de l'audit*». La notification mentionne à cet égard que «*...pour la même raison, la logique conduisant au résultat de l'évaluation des risques ne sera pas révélée. Il ne s'agit cependant pas d'une restriction de l'article 13, puisque le système se contente d'accompagner des décisions, et non de les automatiser*».

S'agissant des données obtenues par les prestataires commerciaux auprès de sources publiques externes, conformément à la notification (telle que remise le 29 novembre 2013), le système sera mis à jour:

- trimestriellement, avec un nouvel ensemble de données provenant du prestataire commercial (c'est-à-dire basé sur les comptes annuels de bénéficiaires et permettant à la Commission d'en tenir compte dans la notation suivante du risque);
- hebdomadairement, avec de nouvelles données provenant des États membres (par SFC ou par la boucle de rétroaction). Les États membres ne peuvent modifier la notation du risque ou d'autres données importées directement dans ARACHNE, mais ils peuvent ajouter un commentaire dans ARACHNE pour conserver une trace de toutes les demandes présentées par la personne concernée.
- Lorsqu'un utilisateur ARACHNE, c'est-à-dire la Commission ou un État membre, identifie une erreur ou une incohérence (information incorrecte sur la direction, information incorrecte sur les actionnaires, information incorrecte dans la presse/les médias, concordances de noms incorrectes entre des sources de données) dans les données externes, il peut le signaler à *VADIS SA/NV* dans le cadre d'une procédure appelée «boucle de rétroaction». Les rectifications apportées par *VADIS SA/NV* via la «boucle de rétroaction» auront un impact sur le système ARACHNE, mais pas sur la source initiale de l'information elle-même. Selon la notification, «*la personne concernée doit demander à connaître la source de l'information si elle a besoin que ses droits soient conférés au-delà du système ARACHNE*».

Dans la déclaration relative à la protection des données, les personnes concernées sont également informées du fait qu'elles peuvent contacter le délégué à la protection des données de la Commission (dont l'adresse électronique est communiquée) en cas de difficultés ou de questions liées au traitement de ces données, et qu'elles peuvent trouver de plus amples informations sur ce traitement de données à caractère personnel dans le Registre public des notifications en indiquant le numéro de notification 3580.

S'agissant de la **conservation des données**, celles-ci sont conservées pendant trois ans à compter de la fin d'un programme opérationnel et conformément aux exigences de l'article 90 du règlement n° 1083/2006. Conformément à la déclaration relative à la protection des données, les données ne seront pas conservées à des fins statistiques.

Définition de l'architecture technique prévue du système: (...).

3. ANALYSE JURIDIQUE

3.1. Contrôle préalable

Les traitements notifiés constituent un traitement de données à caractère personnel («*toute information concernant une personne physique identifiée ou identifiable*») au sens de l'article 2, point a), du règlement (CE) n° 45/2001 (désigné ci-après «le règlement»). Le traitement est réalisé par un organe de l'Union européenne dans le cadre d'activités relevant du champ d'application des traités. Le traitement des données est effectué, du moins en partie, de façon automatique. Le règlement est donc applicable.

Aux termes de l'article 27, paragraphe 1, du règlement, 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*» sont soumis au contrôle préalable du CEPD. L'article 27, paragraphe 2, du règlement dresse une liste non exhaustive des traitements susceptibles de présenter de tels risques. Le point a) mentionne entre autres le traitement de données relatives à des suspicions, infractions ou condamnations pénales. Le point b) cite les traitements destinés à évaluer des aspects de la personnalité des personnes

concernées, tels que leur comportement. Le point c) fait référence aux traitements permettant d'établir un lien entre des données initialement traitées pour des finalités différentes qui ne sont pas prévues dans le droit national ou communautaire. Enfin, le point d) soumet à un contrôle préalable les traitements visant à exclure des personnes d'un contrat. Dans la notification, tous ces points ont été mentionnés comme des motifs de contrôle préalable.

Lors de la réunion du 9 janvier 2014, la Commission a explicitement confirmé qu'ARACHNE ne visait pas à évaluer le comportement individuel particulier de bénéficiaires de fonds au sens de l'article 27, paragraphe 2, point b). Toutefois, comme indiqué au point 2 ci-dessus, des données à caractère personnel liées à des (suspicions d') infractions au sens de l'article 27, paragraphe 2, point a), peuvent être traitées (liste des sanctions par WORLD COMPLIANCE). Pour cette raison, le traitement fait l'objet d'un contrôle préalable.

La notification du DPD a été reçue le 17 mai 2013. Le CEPD a envoyé le projet d'avis au DPD pour observations le 18 novembre 2013. Le CEPD a reçu une réponse le 26 novembre 2013, ainsi qu'une notification révisée et une déclaration relative à la protection des données le 29 novembre 2013. Par la suite, le CEPD a demandé la tenue d'une réunion le 9 décembre 2013; celle-ci a eu lieu le 9 janvier 2014 et a été suivie de la présentation de nouveaux documents le 17 janvier 2014. Un projet d'avis révisé a été envoyé/transmis au DPD pour observations le 24 janvier 2014. Conformément à l'article 27, paragraphe 4, du règlement, le présent avis doit être rendu dans un délai de deux mois. Au total, la procédure a été suspendue pendant 216 jours. Compte tenu de toutes les périodes de suspension, l'avis doit être rendu au plus tard le 17 février 2014.

3.2. Licéité du traitement

Conformément à l'article 5, point a), du règlement[6], il convient de procéder à un test en deux temps pour déterminer: (1) si le traité ou d'autres actes juridiques prévoient une mission d'intérêt public sur la base de laquelle intervient le traitement (base légale) et (2) si les traitements effectués sont réellement nécessaires à l'exécution de cette mission.

Dans la notification, la Commission cite comme possibles bases légales les dispositions du règlement n° 1083/2006 et du règlement n° 1828/2006, la Communication de la Commission sur la stratégie antifraude et le règlement n° 966/2012. Plusieurs de ces dispositions ne constituent pas des bases légales appropriées pour le traitement notifié, ainsi qu'il sera exposé ci-dessous:

- Le **règlement n° 966/2012** contient les règles financières applicables au budget général de l'Union. Les activités de la Commission en rapport avec ARACHNE ne pourraient pas être prévues sur la seule base de son texte. Par exemple, les personnes concernées ne pourraient pas comprendre dans quelle mesure des données à caractère personnel les concernant pourraient être collectées et traitées dans le cadre d'ARACHNE. Le règlement n° 966/2012 est, en tant que tel, trop général pour constituer une base légale au sens de l'article 5, point a);

- **Règlement n° 1083/2006**: l'article 60, point c), du règlement n° 1083/2006 dispose que l'autorité de gestion est responsable, en particulier, de «*s'assurer qu'il existe un système d'enregistrement et de stockage sous forme informatisée des pièces comptables pour chaque opération au titre du programme opérationnel et que les données relatives à la*

[6] L'article 5, point a), du règlement autorise un traitement qui est «*nécessaire à l'exécution d'une mission effectuée dans l'intérêt public sur la base des traités instituant les Communautés européennes ou d'autres actes législatifs adoptés sur la base de ces traités*».

mise en œuvre nécessaires à la gestion financière, au suivi, aux vérifications, aux audits et à l'évaluation sont collectées; ...». Conformément à l'article 61, point e), du règlement n° 1083/2006, l'autorité de certification d'un programme opérationnel est responsable, entre autres, de «*tenir une comptabilité informatisée des dépenses déclarées à la Commission...*». Tandis que les deux articles font référence à un système de contrôle informatisé, ils donnent pouvoir de l'exploiter à l'autorité de gestion et de certification, c'est-à-dire aux entités des États membres conformément à l'article 59, point a), du règlement n° 1083/2006, et non à la Commission. Le CEPD considère cependant que la base légale aux fins de l'article 5, point a), doit se trouver dans des dispositions légales directement applicables à la Commission.

L'article 66 du règlement n° 1083/2006 relève que, aux fins de garantir la qualité de la mise en œuvre du programme opérationnel, «*les échanges de données (...) entre la Commission et les États membres se font par voie électronique, conformément aux modalités d'application du présent règlement adoptées par la Commission conformément à la procédure visée à l'article 103, paragraphe 3*». Si cet article peut servir de base légale à l'actuelle infrastructure SFC2007 (méthode de mise en place de services web) pour la transmission des données opérationnelles des projets depuis les autorités de gestion des États membres vers la Commission, il ne mentionne pas l'objectif de prévention de la fraude poursuivi par ARACHNE.

- **Règlement n° 1828/2006**: conformément à l'article 19, paragraphe 1, du règlement n° 1828/2006, aux fins de l'article 90 du règlement (CE) n° 1083/2006 (intitulé «*Disponibilité des documents*»), «*... l'autorité de gestion assure la mise à disposition d'un registre où sont consignées l'identité et la localisation des organismes détenant les pièces justificatives relatives aux dépenses et aux audits et qui contient tous les documents nécessaires à l'établissement d'une piste d'audit adéquate*». Lorsque des documents n'existent qu'en version électronique, l'article 19, paragraphe 6, du règlement n° 1828/2006 dispose que «*les systèmes informatiques utilisés doivent respecter des normes de sécurité reconnues garantissant que les documents conservés sont conformes aux prescriptions légales nationales et sont fiables à des fins d'audit*». Si ces articles font référence à un système de contrôle informatisé, ils donnent pouvoir de l'exploiter à l'autorité de gestion, c'est-à-dire aux entités des États membres, et non à la Commission. Le CEPD considère cependant que la base légale aux fins de l'article 5, point a), doit se trouver dans des dispositions légales directement applicables à la Commission.

  L'**article 34** du règlement n° 1828/2006 dispose que la «*Commission peut utiliser toutes les informations de nature générale ou opérationnelle communiquées par les États membres en application du présent règlement pour effectuer des analyses de risques et élaborer, sur la base des informations obtenues, des rapports et des dispositifs d'alerte permettant une détection plus efficace des risques*» (mis en exergue par l'auteur). La **section 7** du règlement n° 1828/2006 («*Échange de données par voie électronique*») prévoit la mise en place d'un système informatisé pour l'échange de données comme outil d'échange de l'ensemble des données liées au programme opérationnel (article 39, paragraphe 1) qui «*est accessible aux États membres et à la Commission, soit directement, soit par l'intermédiaire d'une interface assurant la synchronisation et l'enregistrement automatiques des données avec les systèmes informatiques de gestion nationaux, régionaux et locaux*» (article 42, paragraphe 1).

  Si cet article peut sembler être une base légale suffisante pour développer des outils informatisés d'évaluation des risques, il est circonscrit par la limitation aux informations

obtenues des États membres *dans le contexte de l'infrastructure SFC2007 actuelle* (méthode de mise en place de services web) pour la transmission des données opérationnelles de projets depuis les autorités de gestion des États membres vers la Commission («*sur la base des informations obtenues...*»). Or, ARACHNE va au-delà de ces informations puisque, selon la notification, les données du projet seront aussi complétées par des informations provenant de sources publiques. L'article 34 du règlement n° 1828/2006 n'est donc pas une base légale exhaustive au sens de l'article 5, point a), pour le système ARACHNE.

- La **Communication** de la Commission **sur la stratégie antifraude** indique, au chapitre 2.2.3, que «*Les services évalueront la nécessité d'améliorer l'évaluation du risque de fraude en élaborant une procédure plus systématique et formalisée en vue de la mise en évidence des domaines présentant un risque de fraude. Parallèlement, en exploitant les ressources existantes de la manière la plus efficiente possible, il importe que ces mêmes services instaurent des contrôles intelligents s'appuyant sur les outils informatiques, dûment adaptés à leurs besoins, qui ont été développés par certains services en collaboration avec l'OLAF. Ces outils permettent, par exemple, la mise en commun des données existantes relatives à des projets financés par l'UE, clôturés ou en cours. Cette approche se révèle utile à des fins de prévention de la fraude, mais permet également de détecter les cas de plagiat et de double financement frauduleux. Ces outils ne seront pleinement efficaces que si les systèmes d'information pertinents contiennent des données complètes, cohérentes et fiables sur les fonds de l'UE. La possibilité d'analyser des données à des fins de prévention devrait également être prise en considération lors de la définition des exigences opérationnelles imposées aux nouveaux systèmes informatiques*».

Compte tenu de ce qui précède, le CEPD considère que l'association de l'article 34 et de la section 7 du règlement n° 1828/2006, ainsi que du chapitre 2.2.3 de la Communication de la Commission sur la stratégie antifraude, constitue une base légale suffisante aux fins de l'article 5, point a), du règlement.

En outre, les traitements qui font l'objet de la notification semblent nécessaires, en principe, à la détection et à la prévention de la fraude. Sans notations des risques pour identifier les projets les plus risqués et les zones de risque spécifiques résultant de toutes les sources saisissant des informations dans ARACHNE pour un contrôle continu, la Commission ne serait pas capable de détecter et de prévenir la fraude dans la même mesure dans le domaine des Fonds structurels. Il convient toutefois de garder à l'esprit que la nécessité est une question de degré et que la Commission doit s'assurer qu'un tel contrôle n'excède pas ce qui est approprié et proportionné à l'objectif poursuivi. Ces aspects seront analysés au point 3.4 ci-dessous.

3.3. Traitement de catégories particulières de données

L'article 10, paragraphe 1, interdit le traitement de données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, ainsi que le traitement des données relatives à la santé ou à la vie sexuelle. Le traitement de ces catégories particulières de données est interdit, à moins que l'une des exceptions prévues à l'article 10, paragraphe 2, soit applicable. Il convient également de tenir compte de l'article 10, paragraphe 4, du règlement, qui dispose que «*[s]ous réserve de garanties appropriées, et pour un motif d'intérêt public important, des dérogations autres que celles prévues au paragraphe 2 peuvent être prévues par les traités instituant les Communautés européennes ou d'autres actes législatifs adoptés sur la base de*

ces traités ou, si cela s'avère nécessaire, sur décision du contrôleur européen de la protection des données».

Il ressort de la notification que le responsable du traitement n'a pas identifié de catégories particulières de données parmi celles mentionnées à l'article 10, paragraphe 1[7].

Toutefois, même si le traitement de catégories particulières de données n'est pas la finalité principale du traitement, la possibilité du traitement de telles données ne saurait être exclue. Par exemple, l'utilisation de la liste des sanctions pourrait bien révéler des opinions politiques ou des convictions religieuses ou philosophiques. Dans ce cas, le CEPD rappelle que l'interdiction prévue par l'article 10, paragraphe 1, doit être respectée ou qu'il convient de déterminer de façon restrictive s'il est nécessaire d'appliquer une exception. En tout état de cause, les destinataires doivent être informés de cette règle et éviter le traitement de catégories particulières de données, à moins que l'une des exceptions prévues à l'article 10, paragraphe 2 ou 4, ne soit applicable.

L'article 10, paragraphe 5, ne permet le «*traitement de données relatives aux infractions, aux condamnations pénales ou aux mesures de sûreté [...] que s'il est autorisé par les traités [...] ou d'autres actes législatifs adoptés sur la base de ces traités ou, si cela s'avère nécessaire, par le contrôleur européen de la protection des données, sous réserve des garanties spécifiques et appropriées*». Le règlement n° 1828/2006 ou l'un quelconque des autres actes législatifs invoqués comme base légale dans la notification ne semble pas contenir de référence spécifique au fait que la Commission collecterait et traiterait des données relatives à des infractions au sens de l'article 10, paragraphe 5. Cependant, si la Communication de la Commission sur la stratégie antifraude[8] n'est pas un acte législatif, elle applique les obligations qui incombent à la Commission en vertu de l'article 32, paragraphe 4, point a), du règlement n° 966/2012 de mettre en œuvre «*une stratégie appropriée de gestion et de contrôle des risques, coordonnée entre les acteurs compétents de la chaîne de contrôle*» et en vertu de l'article 60, point c), du règlement n° 1083/2006 de s'assurer «*qu'il existe un système d'enregistrement et de stockage sous forme informatisée des pièces comptables pour chaque opération au titre du programme opérationnel et que les données relatives à la mise en œuvre nécessaires à la gestion financière, au suivi, aux vérifications, aux audits et à l'évaluation sont collectées*». Ces obligations sont reflétées plus largement dans les articles 325 et 317 du TFUE.

Le CEPD suggère donc à la Commission d'envisager l'adoption d'une base légale plus spécifique (une décision prise au niveau administratif approprié) l'autorisant à traiter des données aux termes de l'article 10, paragraphe 5, en application des dispositions pertinentes

[7] La notification, à l'égard des PPE et des membres de leur famille et proches associés, précise qu'«*aucune affiliation à un parti ni aucune autre donnée interdite par l'article 10 du règlement n° 45/2001 ne sera traitée (par exemple, le nom du président d'un État peut être traité pour son rôle officiel, mais pas pour son appartenance à un parti politique donné)...*».

[8] Dans ce chapitre, il est expressément indiqué que «*Les services évalueront la nécessité d'améliorer l'évaluation du risque de fraude en élaborant une procédure plus systématique et formalisée en vue de la mise en évidence des domaines présentant un risque de fraude. Parallèlement, en exploitant les ressources existantes de la manière la plus efficiente possible, il importe que ces mêmes services instaurent des contrôles intelligents s'appuyant sur les outils informatiques, dûment adaptés à leurs besoins, qui ont été développés par certains services en collaboration avec l'OLAF. Ces outils permettent, par exemple, la mise en commun des données existantes relatives à des projets financés par l'UE, clôturés ou en cours. Cette approche se révèle utile à des fins de prévention de la fraude, mais permet également de détecter les cas de plagiat et de double financement frauduleux. Ces outils ne seront pleinement efficaces que si les systèmes d'information pertinents contiennent des données complètes, cohérentes et fiables sur les fonds de l'UE. La possibilité d'analyser des données à des fins de prévention devrait également être prise en considération lors de la définition des exigences opérationnelles imposées aux nouveaux systèmes informatiques*».

des règlements n° 966/2012 et n° 1083/2006. Le traitement de catégories particulières de données devrait, en tout état de cause, être limité à ce qui est nécessaire au respect des obligations légales relatives aux deux règlements. Des garanties appropriées pour veiller au respect des principes de nécessité, de proportionnalité et de qualité des données devraient être énoncées à cet égard (voir également le point 3.4 ci-dessous).

3.4. Traitement de données à caractère personnel pour le compte du responsable du traitement

VADIS SA/NV, en qualité de sous-traitant, prend en charge le processus de collecte et de préparation des données. Cette activité est régie par un contrat écrit stipulant en particulier, à son annexe I, article II.6, que le sous-traitant agit sur les instructions du responsable du traitement, et qui contient des clauses écrites énonçant les obligations prévues aux articles 21 et 22 du règlement qui incombent au sous-traitant.

En principe, la Commission se conforme donc à l'article 23 du règlement. Néanmoins, le CEPD serait favorable à une clause relative à la protection des données concernant exclusivement les obligations du sous-traitant. Le sous-traitant devrait plutôt être informé des conditions liées au traitement de ses données par la Commission au moyen d'une déclaration relative à la protection des données. De plus, une clause spécifique relative à la protection des données pourrait être bénéfique à un traitement impliquant une technologie complexe (voir, par exemple, notre recommandation au point 3.6).

3.5. Qualité des données

L'article 4, paragraphe 1, point c), du règlement dispose que 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. Cela comprend le fait que les données doivent être tenues exactes et à jour; toutes les mesures raisonnables doivent être prises pour que les données inexactes ou incomplètes soient rectifiées ou supprimées (article 4, paragraphe 1, point d), du règlement).

En l'espèce, il existe des motifs raisonnables de présumer que certaines catégories de données seront de qualité suffisante, telles que les données d'identification fournies par les personnes concernées elles-mêmes aux autorités de gestion du FSE et du FEDER (disponibles dans ARACHNE via l'infrastructure SFC2007) ou les extraits des listes des sanctions et d'application.

On ne peut en dire de même des données provenant de sources publiques externes. Dans le contexte du traitement en cause, celles-ci sont obtenues auprès de deux prestataires commerciaux (qui lisent entre autres des journaux et magazines à la recherche d'informations pertinentes sur les risques). Sur ce point, la Commission doit prendre des mesures appropriées pour garantir un niveau d'exactitude élevé.

a) Le CEPD se réjouit de l'existence de la procédure appelée «boucle de rétroaction». Le CEPD relève cependant que, selon la notification, un utilisateur ARACHNE identifiant une erreur ou irrégularité dans les données extérieures *peut* la signaler à *VADIS SA/NV*. Il ne semble donc pas y avoir d'*obligation* pour les utilisateurs d'ARACHNE de signaler des erreurs ou irrégularités. Cela n'est pas suffisant pour garantir un degré approprié d'exactitude des données à caractère personnel. Le CEPD recommande que le signalement à *VADIS SA/NV* d'erreurs ou d'irrégularités au niveau des données externes devienne obligatoire pour les utilisateurs d'ARACHNE.

b) S'agissant des informations dérivées de sources médiatiques externes, le CEPD comprend que la «*personne concernée doit demander à connaître la source de l'information si elle a besoin que ses droits soient conférés au-delà du système ARACHNE*» (mis en exergue par l'auteur). Le CEPD reconnaît que l'octroi de droits d'accès et de rectification dans le contexte du système ARACHNE ne va pas *au-delà* de ce système.

Toutefois, pour les informations dérivées de sources médiatiques externes, le CEPD recommande à la Commission d'élaborer et mettre en œuvre des mesures efficaces dans le contexte de ses rapports contractuels avec le sous-traitant (*VADIS SA/NV*), afin de garantir un niveau élevé de qualité des données allant au-delà de la procédure appelée «boucle de rétroaction». Ces mesures pourraient par exemple couvrir les domaines suivants[9]:

- les personnes chargées du contrôle des sources médiatiques externes devraient recevoir une formation quant à la façon de faire tout en respectant les exigences en matière de protection des données, en particulier l'application stricte et claire du principe de limitation des finalités;
- une description expliquant si et comment l'entité fait la distinction entre les données factuelles, les données subjectives, les informations des services de renseignement et les données collectées au sujet de différentes catégories de personnes concernées;
- d'autres étapes devraient inclure l'abstention d'utilisation de reportages peu fiables et la vérification par recoupement, auprès de sources indépendantes fiables, des informations obtenues dans des reportages.

3.6. Conservation des données

Comme cela a été souligné dans la partie 2 du présent avis, les données sont conservées pendant trois ans, conformément aux exigences de l'article 90 du règlement n° 1083/2006, et aucun traitement ultérieur n'est prévu à des fins statistiques. Dans ce contexte, le CEPD n'a pas de raison de penser que des données à caractère personnel seront conservées sous une forme permettant l'identification de personnes concernées pendant une durée excédant celle nécessaire à la réalisation des finalités pour lesquelles les données sont collectées et/ou pour lesquelles elles sont traitées ultérieurement au sens de l'article 4, paragraphe 1, point e), du règlement. Le CEPD tient néanmoins à recommander d'imposer à *VADIS SA/NV* de supprimer des données à caractère personnel à la fin de la période de conservation fixée dans le contrat écrit conclu.

3.7. Transfert de données

Les transferts de données à des destinataires soumis au règlement sont régis par l'article 7 de ce dernier; les transferts à des destinataires soumis à la législation nationale transposant la directive 95/46/CE sont régis par l'article 8 du règlement.

- L'article 7, paragraphe 1, dispose que les données ne peuvent faire l'objet de transferts entre institutions ou organes communautaires ou en leur sein que si elles sont «*nécessaires à l'exécution légitime de missions relevant de la compétence du destinataire*». Les transferts visés à l'article 7 interviennent aussi bien au sein de la Commission qu'à destination d'autres institutions ou organes communautaires. Des transferts internes peuvent intervenir dans la mesure nécessaire pour prendre des décisions de financement et pour des fonctions de contrôle interne. Selon la notification,

[9] Voir recommandations similaires dans l'avis du CEPD dans le dossier 2012-0326 au sujet du traitement de données LBC-FT de la Banque européenne d'investissement.

les transferts vers d'autres institutions ou organes communautaires concernent des transferts à l'OLAF et à la Cour des comptes européenne. Dans la mesure où ces transferts concernent une enquête réalisée au sujet de dossiers spécifiques, ils relèvent en principe de l'article 7, paragraphe 1, du règlement. Une analyse au cas par cas doit toutefois être réalisée pour déterminer si les conditions du transfert sont effectivement réunies.

- Les transferts vers les autorités de gestion et leurs organes intermédiaires dans les États membres, leurs autorités de certification et les autorités d'audit sont soumis à l'article 8 du règlement. L'article 8, point a), autorise les transferts de données à caractère personnel à de tels destinataires «*si le destinataire démontre que les données sont nécessaires à l'exécution d'une mission effectuée dans l'intérêt public ou relevant de l'exercice de l'autorité publique*». Cet article couvre les transferts vers les autorités des États membres dans le contexte de la détection et de la prévention de la fraude conformément à la Communication de la Commission sur la stratégie antifraude.

Selon la notification, aucun transfert au titre de l'article 9 du règlement, par exemple vers des pays tiers, n'est prévu.

3.8. Droits d'accès et de rectification

Les articles 13 et 14 du règlement disposent que les personnes concernées peuvent à tout moment accéder aux données conservées les concernant et les modifier.

Dans la notification, la Commission indique que ces droits peuvent être limités conformément à l'article 20, paragraphe 1, point b), du règlement. Le CEPD souligne que toute restriction aux droits d'accès et de rectification ne peut être opérée qu'au cas par cas et uniquement dans la mesure où elle est *nécessaire* à cette fin. Des procédures appropriées doivent être mises en place pour permettre l'exercice de ces droits dans de telles situations. En tout état de cause, l'article 20, paragraphe 3, du règlement doit être respecté par la Commission: «[s*i*] *une limitation prévue au paragraphe 1 est imposée, la personne concernée est informée conformément au droit communautaire des principales raisons qui motivent cette limitation et de son droit de saisir le contrôleur européen de la protection des données*».

Selon la déclaration relative à la protection des données, le «*droit d'accès des personnes concernées conformément à l'article 13 sera apprécié au cas par cas et reporté s'il pourrait donner des opportunités à de potentiels fraudeurs de trouver des faiblesses dans le processus d'évaluation des risques et de les contourner. Un accès sera accordé une fois prise la décision de ne pas réaliser d'audit ou à la date de réalisation de l'audit*».

À la lumière de cette explication fournie aux personnes concernées, le CEPD prend note de l'approche au cas par cas et ne voit aucune raison de croire que la Commission applique des restrictions aux droits d'accès et de rectification pendant une durée plus longue que nécessaire.

3.9. Information de la personne concernée

Lorsque les données ne sont pas collectées auprès de la personne concernée, comme c'est le cas du système ARACHNE, les informations fournies aux personnes concernées doivent comprendre au moins les éléments suivants (voir l'article 12 du règlement):

- identité du responsable du traitement;

- finalités du traitement;
- destinataires ou catégories de destinataires;
- catégories de données collectées;
- existence des droits d'accès et de rectification;
- base légale du traitement;
- durées de conservation;
- droit de saisir le CEPD;
- origine des données, sauf si le responsable du traitement ne peut divulguer cette information pour des raisons de secret professionnel.

En ce qui concerne les moyens de communication de ces informations, le CEPD considère que la publication de la déclaration relative à la protection des données sur le site web du Fonds social européen ne suffit pas, à elle seule, à garantir que les personnes concernées reçoivent effectivement l'information. En réalité, les informations publiées sur le site web ne seront pas accessibles à toutes les personnes potentiellement concernées. Le CEPD considère donc que cette publication doit être complétée, dans la mesure du possible, par une certaine forme d'information individuelle contenant les éléments nécessaires conformément à l'article 12 du règlement.

Lorsque des données sont obtenues auprès des autorités de gestion du FSE et du FEDER (via l'infrastructure SFC2007), elles ont été préalablement collectées auprès des personnes concernées elles-mêmes, au moins partiellement. Le CEPD recommande donc de fournir l'information nécessaire conformément à l'article 12 du règlement sur ce point.

3.10. Décisions individuelles automatisées

L'article 19 du règlement dispose que «*[l]a personne concernée a le droit de ne pas être soumise à une décision produisant des effets juridiques à son égard ou l'affectant de manière significative, prise sur le seul fondement d'un traitement automatisé de données destiné à évaluer certains aspects de sa personnalité, tels que son rendement professionnel, sa fiabilité ou son comportement, sauf si cette décision est expressément autorisée en vertu de la législation nationale ou communautaire ou, si cela s'avère nécessaire, par le contrôleur européen de la protection des données. Dans les deux cas, des mesures garantissant la sauvegarde des intérêts légitimes de la personne concernée doivent être prises, telles que des mesures lui permettant de faire valoir son point de vue*».

Selon la notification et comme cela a été confirmé explicitement lors de la réunion du 9 janvier 2014, aucune décision automatisée ne sera prise exclusivement sur la base des indicateurs de risques produits par ARACHNE, puisque le système ne permet pas automatiquement de conclure à une erreur ou une irrégularité[10].

3.11. Mesures de sécurité

(...)

[10] La notification mentionne d'ailleurs explicitement que «*...la logique conduisant au résultat de l'évaluation des risques ne sera pas révélée. Il ne s'agit cependant pas d'une restriction de l'article 13, puisque le système se contente d'accompagner des décisions, et non de les automatiser*».

4. CONCLUSION

Il n'y aucune raison de penser qu'il existe une violation des dispositions du règlement (CE) n° 45/2001 pour autant qu'il soit pleinement tenu compte des observations apportées dans le présent avis. En particulier, la Commission doit:

- Envisager l'adoption d'une base légale plus spécifique (une décision prise au niveau administratif approprié) autorisant la Commission à traiter des données conformément à l'article 10, paragraphe 5, du règlement en application des dispositions pertinentes des règlements n° 966/2012 et n° 1083/2006. Le traitement de catégories particulières de données devrait, en tout état de cause, être limité à ce qui est nécessaire au respect des obligations légales relatives aux deux règlements. Des garanties appropriées pour veiller au respect des principes de nécessité, de proportionnalité et de qualité des données concernant la nécessité, la proportionnalité et la qualité des données devraient être énoncées à cet égard;
- Dans le contexte de la «boucle de rétroaction», rendre obligatoire le signalement à *VADIS SA/NV* par les utilisateurs d'ARACHNE de toute erreur ou incohérence identifiée dans les données externes;
- Développer et mettre en œuvre des mesures effectives garantissant un haut niveau de qualité des données concernant les informations dérivées de sources médiatiques externes conformément aux recommandations formulées au point 3.4 ci-dessus;
- S'assurer que les transferts à l'OLAF et à la Cour des comptes européenne en vertu de l'article 7 du règlement interviennent selon une analyse au cas par cas;
- Imposer à *VADIS SA/NV* de supprimer des données à caractère personnel à la fin de la période de conservation fixée dans le contrat écrit conclu;
- S'agissant des données obtenues auprès des autorités de gestion du FSE et du FEDER (via l'infrastructure SFC2007), fournir les informations nécessaires sur les traitements dans le cadre du système ARACHNE conformément à l'article 12 du règlement lorsque les données ont initialement été collectées auprès des personnes concernées elles-mêmes;
- Revoir les procédures de gestion des utilisateurs afin d'y intégrer un examen de tous les comptes utilisés par le système ARACHNE et donner des conseils aux États membres pour promouvoir une approche cohérente en termes de gestion des utilisateurs.

Fait à Bruxelles, le 17 février 2014

(signé)

Giovanni BUTTARELLI