



## **Avis de contrôle préalable**

«Procédure de lancement d’alerte au sein de Fusion for Energy»  
Dossier 2016-0087

\*\*\*

Les procédures de lancement d’alerte fournissent des filières sûres permettant au personnel ou aux autres informateurs de signaler les fraudes, corruptions et autres manquements graves survenus au sein des organisations. Dans le cadre de procédures de ce type, un traitement d’informations à caractère personnel aura lieu, par exemple, pour les personnes soupçonnées de manquements et les informateurs et/ou les parties tierces, telles que les témoins.

\*\*\*

Bruxelles, le 31 mars 2016

## 1. Procédure

Le 26 janvier 2016, le Contrôleur européen de la protection des données (ci-après le «CEPD») a reçu une notification de contrôle préalable de la part du délégué à la protection des données (ci-après le «DPD») de Fusion for Energy (ci-après «F4E») concernant la procédure de lancement d'alerte au sein de F4E.

Conformément à l'article 27, paragraphe 4, du règlement 45/2001 (ci-après le «règlement»), le présent avis doit être rendu dans un délai de deux mois, sans compter les suspensions pour demandes d'informations complémentaires<sup>1</sup>.

## 2. Les faits

L'**objectif** de cette procédure est de permettre le signalement de «graves irrégularités», à savoir les activités illégales, notamment les fraudes, corruptions, fautes professionnelles ou autres manquements graves au sein de F4E. Pour cela, il est nécessaire de mettre en place des canaux de communication pour les lanceurs d'alerte, de gérer et de suivre les informations communiquées, mais aussi de garantir des mécanismes de protection ainsi que des voies de recours adéquates pour les lanceurs d'alerte. Cette notification couvre également le traitement de données au sein de F4E, dans l'éventualité où l'OLAF contacterait l'organisation pour une demande d'information (car l'alerte relative à une irrégularité survenue au sein de F4E aura été lancée directement auprès de l'OLAF).

Les **informations à caractère personnel traitées** sont contenues dans le rapport présenté par le lanceur d'alerte et dans tout document élaboré ultérieurement en réponse à ce premier rapport. Ces documents peuvent notamment comporter des noms, des coordonnées et d'autres données à caractère personnel. Lorsque le rapport contiendra des informations à caractère personnel qui ne sont à l'évidence pas pertinentes pour l'examen des questions soulevées dans le rapport, ces informations seront supprimées dès que possible, après consultation du lanceur d'alerte, pour autant que cela n'ait pas pour effet de retarder indûment l'examen sur le fond.

Les informations sont fournies par le biais d'une **déclaration de confidentialité** publiée sur l'intranet de F4E. En outre, la déclaration de confidentialité sera également fournie à tout membre du personnel concerné par une procédure de lancement d'alerte donnée, et ce dès que possible. Toutefois, s'il existe un risque sérieux que la capacité de F4E à enquêter efficacement sur les allégations ou à recueillir les éléments de preuve nécessaires soit compromise par une notification, cette dernière peut être différée tant que ce risque persiste.

Il est mentionné dans la notification que les informations à caractère personnel seront **divulguées** en fonction du strict besoin d'en connaître. Cette divulgation dépendra de la question de savoir s'il est nécessaire que F4E examine le dossier en question ainsi que le canal de communication choisi par le lanceur d'alerte, et si ce dernier souhaite recevoir des conseils préalables.

En ce qui concerne la **période de conservation**, les dossiers qui ne conduisent pas à l'ouverture d'une enquête administrative ou d'une procédure disciplinaire, c'est-à-dire les dossiers portant sur des alertes jugées non fondées par F4E ou l'OLAF, doivent être supprimés dans les plus brefs délais à compter de la date à laquelle F4E décide de clore le dossier sans autre forme de suivi et au plus tard deux mois après une telle décision. Les dossiers motivant l'ouverture d'une enquête administrative ou d'une procédure disciplinaire

---

<sup>1</sup> Le dossier a été suspendu du 18 mars 2016 au 23 mars 2016 dans l'attente d'observations de la part du DPD. Le CEPD est dès lors tenu de rendre un avis pour le 31 mars 2016 au plus tard.

seront conservés pendant une durée conforme aux délais de conservation prévus pour ces dossiers par la procédure concernée.

En ce qui concerne les **mesures de sécurité**  
[...]

### **3. Analyse juridique**

#### **3.1. Contrôle préalable**

Le traitement de données à caractère personnel est effectué par une agence de l'Union européenne. En outre, le traitement est partiellement effectué à l'aide de procédés automatisés. Par conséquent, le règlement est applicable.

Ce traitement est soumis à un contrôle préalable car il présente des risques particuliers. En effet, F4E traitera des informations relatives à des suspicions d'infractions en lien avec des fraudes potentielles et procédera à une évaluation de la conduite des personnes accusées de manquement<sup>2</sup>.

#### **3.2. Qualité des données et catégories particulières de données**

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. Elles doivent aussi être exactes et, si nécessaire, mises à jour (article 4, paragraphe 1, point d)).

Il est possible que F4E reçoive, peut-être involontairement, des informations ne présentant aucun intérêt ou aucune pertinence pour l'enquête et qui concernent également des catégories particulières de données<sup>3</sup>. Les données à caractère personnel et, en particulier, les catégories particulières de données qui ne sont à l'évidence pas pertinentes aux fins d'enquêter sur une fraude ou autre manquement grave dans le cadre d'une procédure de lancement d'alerte ne devraient pas être traitées davantage.

Le CEPD se félicite du fait que les informations à caractère personnel qui ne présentent aucune pertinence seront supprimées du rapport par F4E, et ce dès que possible. Il est de **bonne pratique** d'émettre une recommandation générale à l'intention des personnes chargées de traiter les dossiers, par exemple dans le règlement intérieur de procédure, leur **rappelant les exigences en matière de qualité des données et leur recommandant de veiller au respect des règles**.

#### **3.3. Informations transmises aux personnes**

Les articles 11 et 12 du règlement énumèrent les informations minimales à fournir aux personnes impliquées dans un dossier en ce qui concerne le traitement de données à caractère personnel.

---

<sup>2</sup> L'article 27 du règlement soumet au contrôle préalable du CEPD 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 énumère les traitements susceptibles de présenter de tels risques, et notamment au point a), les traitements de données relatives à des suspicions d'infractions et au point b), les traitements destinés à évaluer des aspects de la personnalité des personnes concernées, tels que leur comportement.

<sup>3</sup> Article 10 du règlement.

En ce qui concerne les procédures permettant notamment aux personnes concernées d'exercer leurs droits (d'accès, de rectification et autres), il est de bonne pratique d'inclure des informations concernant le délai dans lequel une réponse peut être donnée (par exemple, 3 mois pour les demandes d'accès, sans délai pour les demandes de rectification, etc.).

Le CEPD souligne que, lorsque F4E décide d'appliquer une limitation en matière d'information, de droit d'accès, de droit de rectification, etc. au titre de l'article 20, paragraphe 1, du règlement, ou de différer l'application de l'article 20, paragraphes 3 et 4<sup>4</sup>, cette décision doit être prise au cas par cas exclusivement. Dans tous les cas, F4E doit être en mesure d'apporter des preuves qui contiennent des raisons détaillées motivant cette décision (à savoir une décision motivée). Ces raisons doivent démontrer, par exemple, qu'il existe un risque élevé qu'un tel accès entrave la procédure ou porte atteinte aux droits et libertés d'autrui, et doivent être étayées avant qu'il soit décidé d'appliquer quelque limitation ou report que ce soit. F4E doit s'assurer que les raisons dûment documentées sont mises à la disposition du CEPD s'il en fait la demande dans le cadre d'une mesure de surveillance et d'application.

### **3.4. Mesures de sécurité**

[...]

## **4. Conclusion**

En vue de respecter le règlement, F4E doit:

- veiller à ce que les membres du personnel chargés du traitement des rapports de lancement d'alerte connaissent les exigences en matière de qualité des données (point 3.2.);
- [...]

Veillez informer le CEPD, dans un délai de 3 mois, des mesures prises sur la base des recommandations formulées dans le présent avis.

Fait à Bruxelles, le 31 mars 2016

(signé)

Wojciech Rafał WIEWIÓROWSKI

---

<sup>4</sup> Aux termes de l'article 20, paragraphe 5, du règlement.