

LE CONTRÔLEUR EUROPÉEN  
DE LA PROTECTION DES DONNÉES

RAPPORT  
ENQUÊTE 2015

*Évaluation du respect des règles  
de protection des données au  
sein des institutions de l'UE*



21 Janvier 2016

## TABLE DES MATIÈRES

<b>I.</b>	<b>Avant-propos</b> .....	<b>2</b>
<b>II.</b>	<b>Résumé</b> .....	<b>3</b>
<b>III.</b>	<b>Rapport général</b> .....	<b>4</b>
<b>1.</b>	<b>Introduction</b> .....	<b>4</b>
<b>2.</b>	<b>Résultats comparatifs de l'enquête</b> .....	<b>6</b>
2.1.	INVENTAIRE ET REGISTRE DES TRAITEMENTS. ÉTAT DES NOTIFICATIONS AU CEPD	6
2.2.	TRANSFERTS EN 2013-2014 À DES DESTINATAIRES NON SOUMIS AUX DISPOSITIONS NATIONALES ADOPTÉES EN APPLICATION DE LA DIRECTIVE 95/46/CE .....	12
2.3.	SÉCURITÉ DE L'INFORMATION .....	18
2.4.	GARANTIR L'EFFACEMENT EFFECTIF DES DONNÉES À CARACTÈRE PERSONNEL ....	20
2.5.	VOTRE DÉLÉGUÉ À LA PROTECTION DES DONNÉES ET VOUS .....	21
2.6.	ORGANES QUI N'ONT PAS RÉPONDU À L'ENQUÊTE.....	26
<b>3.</b>	<b>Suivi de l'enquête précédente: visites de contrôle</b> .....	<b>27</b>
3.1.	REMARQUES GÉNÉRALES .....	27
3.2.	EIGE.....	28
3.3.	FEI.....	28
3.4.	CSUE (CENTRE SATELLITAIRE DE L'UE) ET GSA (AGENCE DU GNSS EUROPÉEN).....	28
3.5.	IESUE.....	29
3.6.	ÉVALUATION DU PROGRAMME DES VISITES.....	29
<b>4.</b>	<b>Conclusions et suivi prévu</b> .....	<b>31</b>
<b>IV.</b>	<b>Annexe 1) Méthodologie</b> .....	<b>32</b>
<b>V.</b>	<b>Annexe 2) Limites de la méthodologie</b> .....	<b>33</b>
<b>VI.</b>	<b>Annexe 3) Groupes d'institutions de l'UE</b> .....	<b>34</b>
<b>VII.</b>	<b>Annexe 4) Liste des acronymes des institutions</b> .....	<b>35</b>

## I. Avant-propos

Le Contrôleur européen de la protection des données (CEPD) est l'autorité de contrôle indépendante chargée<sup>1</sup> de surveiller et d'assurer l'application du règlement (CE) n° 45/2001 (le «règlement»)<sup>2</sup>, la législation relative à la protection des données qui s'applique aux institutions, aux organes, aux bureaux et aux agences de l'UE (les «institutions de l'UE») qui traitent des données à caractère personnel.

Les institutions de l'UE collectent, utilisent et conservent des données à caractère personnel aussi bien dans leurs tâches administratives courantes que dans le cadre de leurs activités fondamentales; le CEPD a pour mission de les aider à s'orienter vers une approche non plus basée exclusivement sur le respect mais aussi sur la responsabilisation<sup>3</sup> en étroite coopération avec le délégué à la protection des données (DPD) désigné dans chaque institution de l'UE. Les institutions de l'UE doivent non seulement respecter le règlement mais aussi être en mesure d'en *apporter la preuve*.

En vue de renforcer notre efficacité et parce que nous nous efforçons d'améliorer davantage encore les échanges avec les institutions de l'UE que nous contrôlons, le CEPD effectue tous les deux ans un **état général de la situation** en se concentrant sur les aspects qui donnent une bonne indication des progrès réalisés au regard de la mise en œuvre du règlement dans les institutions de l'UE. Le présent rapport est le résultat du cinquième exercice consécutif; il a été rédigé sur la base des réponses fournies par **61 institutions de l'UE** au plus tard en septembre 2015<sup>4</sup>.

Publié dans le cadre de la politique du CEPD relative à l'application des règles<sup>5</sup>, le présent rapport vise à responsabiliser davantage au respect des règles relatives à la protection des données par les institutions de l'UE. Le rapport s'inscrit dans le cadre de nos efforts qui visent à former et orienter les institutions de l'UE sur la façon de mieux respecter en pratique les règles en matière de protection des données, tout en se concentrant sur les types de traitement qui présentent des risques élevés pour les individus. Le rapport souligne donc les **progrès** réalisés par rapport aux enquêtes précédentes, mais relève également les **manquements**. Il évalue également les résultats des **visites** réalisées dans un certain nombre d'institutions de l'UE sur la base des résultats de l'enquête précédente.

Les réponses reçues et les visites de contrôle réalisées précédemment confirment que la mise en œuvre du règlement n'est pas seulement une question de temps ou de ressources, mais aussi de volonté de l'organisation. Le rapport ne vise donc pas à évaluer les performances individuelles du DPD désigné dans chaque institution de l'UE, mais plutôt les performances globales de chaque institution de l'UE chargée de la protection du droit à la vie privée des individus lors du traitement de données à caractère personnel. Le respect de la réglementation est en effet un processus qui nécessite **l'engagement** et le **soutien** de la direction dans chaque institution de l'UE.

Le CEPD tiendra compte des résultats de la présente enquête au moment de planifier de nouvelles activités de supervision et d'application des règles. Cependant, dans notre activité

---

<sup>1</sup> Conformément à l'article 41, paragraphe 2, du règlement.

<sup>2</sup> Règlement (CE) n° 45/2001 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données.

<sup>3</sup> Voir la Stratégie 2015-2019 du CEPD publiée le 2 mars 2015, disponible sur le site web du CEPD: [https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Strategy/15-02-26\\_Strategy\\_2015\\_2019\\_FR.pdf](https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Strategy/15-02-26_Strategy_2015_2019_FR.pdf).

<sup>4</sup> Plusieurs organes et agences ont répondu après cette date. Dans la mesure du possible, leurs réponses ont néanmoins été intégrées au présent rapport.

<sup>5</sup> Voir le document stratégique du CEPD du 13 décembre 2010 sur «[Contrôler et garantir le respect du règlement \(CE\) n° 45/2001](#)», p. 8.

de supervision des institutions de l'UE, nous agissons par l'éducation, la persuasion et l'exemple, en réservant les pouvoirs d'exécution dont nous sommes investis aux situations de dernier ressort. Nos activités associeront des **orientations** données aux institutions de l'UE, des **mesures d'application des règles** et d'autres initiatives de **responsabilisation**. Plus particulièrement, des visites de contrôle déclenchées par un manque manifeste d'engagement de la part d'une institution ou d'un organe seront planifiées sur la base des résultats de cette enquête.

## II. Résumé

La présente enquête dresse un état des lieux général en ce qui concerne le respect par les institutions de l'UE des règles applicables en matière de protection des données et illustre le rôle du CEPD en tant qu'autorité de contrôle indépendante.

Bien que l'enquête revête un caractère technique et qu'elle soit axée sur des formalités, elle fournit des indications précieuses pour évaluer les tendances, elle favorise la transparence vis-à-vis des parties prenantes et elle alimente les choix du CEPD en ce qui concerne les activités de supervision et de mise en application. La publication de l'enquête est l'occasion pour le CEPD d'arrêter ses activités pour l'année 2016.

Dans l'ensemble, les résultats attestent de progrès constants s'agissant de la mise en œuvre des règles relatives à la protection des données par toutes les institutions de l'UE. L'enquête confirme donc une tendance globalement positive parmi les institutions très hétéroclites de l'UE, dont les traitements varient considérablement du fait de leur portée et de leur complexité.

Les institutions bien établies et matures doivent désormais veiller à maintenir leurs résultats pour ce qui est de la tenue d'inventaires adéquats et du maintien des taux de notification à leur DPO et au CEPD.

Des institutions moins matures ont rattrapé leur retard, plusieurs agences ayant indiqué des taux de notification parfaits. Dans les domaines où les progrès ont connu un ralentissement, notamment en ce qui concerne les notifications au CEPD, nous apporterons aux institutions le soutien nécessaire pour faire en sorte que la protection des données devienne un réflexe.

### III. Rapport général

#### 1. Introduction

En tant qu'administrations publiques, les institutions de l'UE traitent des données à caractère personnel, aussi bien dans le cadre de leurs activités fondamentales que dans leurs tâches administratives.

Il incombe aux institutions de l'UE de protéger les libertés et les droits fondamentaux des personnes physiques pour ce qui est du traitement des données à caractère personnel et de mettre en place des mesures appropriées et effectives afin de garantir le respect des principes et des obligations énoncés dans le règlement (CE) n° 45/2001 (ci-après le «règlement»), et d'en produire la preuve.

C'est le devoir et la tâche du Contrôleur européen de la protection des données (CEPD) de contrôler et de garantir que les droits des individus sont respectés conformément au règlement<sup>6</sup>.

Dans son document stratégique adopté en décembre 2010<sup>7</sup> le CEPD annonce qu'il «*continuera de mener ces enquêtes 'périodiques' afin de garantir qu'il dispose d'un aperçu représentatif du respect de la protection des données au sein des institutions ou organes de l'Union, et qu'il peut fixer des objectifs internes appropriés pour traiter ses constatations*».

Fin avril 2015, le CEPD s'est attelé à son cinquième état de la situation, qui s'inscrit dans le droit fil des exercices réalisés tous les deux ans depuis 2007 et permet donc de décrire l'évolution des tendances en matière de respect de la réglementation.

L'exercice était de grande envergure, puisqu'il couvrait toutes les institutions de l'UE (61), et était axé sur les aspects donnant une bonne indication des progrès réalisés dans la mise en œuvre du règlement par ces dernières. Outre les questions habituelles sur l'état de l'inventaire et du registre, cette édition de l'enquête incluait également des questions sur les transferts relevant de l'article 9 du règlement, sur la sécurité de l'information, sur les mesures prises pour garantir l'effacement effectif des données à caractère personnel à la fin du délai de conservation et sur la participation du DPD à la conception de nouveaux traitements.

Le présent rapport se fonde sur les réponses que 61 institutions de l'Union (notamment celles des anciens deuxième et troisième piliers) ont apportées aux lettres du CEPD soulevant des questions spécifiques. Le CEPD a reçu des réponses de toutes les institutions de l'UE concernées, sauf de l'EC SESAR. Le CEPD abordera cette question de manière spécifique.

Le CEPD tiendra compte des résultats de cet exercice au moment de planifier ses futurs programmes d'activités de supervision et d'application des règles. Ces programmes associeront des orientations données aux institutions de l'UE, des mesures d'application des règles et d'autres initiatives de responsabilisation.

Le rapport est organisé comme suit: la section 2 contient une analyse comparative des réponses apportées à nos lettres, question par question, chacune précédée d'une brève explication sur la pertinence de cette question; la section 3 présente un suivi des visites réalisées en conséquence de l'enquête de 2011; dans la mesure du possible, les résultats obtenus en matière de respect de la réglementation avant et après les visites sont comparés afin d'analyser l'incidence de ces dernières; la section 5 contient une conclusion et un résumé.

---

<sup>6</sup> Conformément à l'article 41, paragraphe 2, du règlement.

<sup>7</sup> Voir le document d'orientation du CEPD du 13 décembre 2010 intitulé «[Contrôler et garantir le respect du règlement n° 45/2001](#)», p. 8.



## 2. Résultats comparatifs de l'enquête

### 2.1. Inventaire et registre des traitements. État des notifications au CEPD

Contrairement aux exercices précédents, le CEPD n'a pas demandé les copies actualisées de l'inventaire ou du registre, mais seulement le *nombre* de traitements concernés 1) identifiés dans l'inventaire, 2) ceux notifiés au DPD et inclus dans le registre, 3) ceux identifiés comme relevant de l'article 27 et 4) ceux ayant déjà fait l'objet d'une notification au CEPD au titre de l'article 27. Lorsque ces informations étaient également disponibles de manière plus détaillée, pour chaque direction générale, par exemple, les institutions ont été invitées à les fournir également.

Une **grande majorité** des institutions de l'UE tiennent **à la fois un inventaire et un registre**, comme le recommande le CEPD. Les institutions de l'UE qui ne tiennent pas d'inventaire distinct ajoutent parfois au registre une section sur les futurs traitements et fusionnent, dans la pratique, les deux documents en un seul (par exemple, le Parlement européen).

Par rapport à la dernière enquête générale réalisée en 2013, **les taux de notification ont augmenté de manière générale**. Les tableaux ci-dessous donnent un aperçu des taux de notification dans la présente enquête et des changements intervenus depuis l'enquête de 2013. La colonne «Article 25» renvoie à tous les traitements, parmi lesquels ceux qui doivent en outre être notifiés au CEPD au titre de l'article 27 du règlement. La colonne «Article 27» fournit des informations distinctes sur ces traitements.

**Dans certains cas, les taux ont diminué.** Cette diminution concerne généralement des institutions de l'UE dont le taux de conformité est élevé, dans des cas où des mises à jour de l'inventaire ont permis aux DPD de découvrir d'autres traitements. Elle peut conduire à des fluctuations entre des valeurs de 90 à 100 % et n'est donc pas préoccupante. Compte tenu de la mise au point constante de nouveaux traitements, il est difficile d'obtenir un taux de notification de 100 % au titre de l'article 25, surtout pour les grandes institutions. Pour les notifications au titre de l'article 27, même un ou deux traitements n'ayant pas encore été notifiés peuvent conduire à ce qui semble être une baisse notable des taux de notification, étant donné que le nombre de traitements par institution a tendance à être assez faible<sup>8</sup>.

L'objectif de ces valeurs de référence est de comparer la performance des institutions de l'UE avec celle de leurs pairs. Il ne serait pas juste de comparer une institution bien établie comme le Conseil ou la Commission à une agence qui vient d'être créée et qui est toujours en cours de croissance ou d'établissement. Pour cette raison, les institutions sont comparées à d'autres

*En vertu des dispositions de l'article 25 du règlement, le DPD reçoit une notification de tous les traitements de données à caractère personnel. En vertu de l'article 26 du règlement, les traitements notifiés sont conservés dans un **registre**, dont le contenu minimum est défini dans cet article. Les traitements considérés comme étant «à risque» au titre de l'article 27 du règlement doivent également être notifiés au CEPD en vue d'un contrôle préalable. En outre, un «**inventaire**» des traitements prévus ou déjà en cours, mais qui n'ont pas encore été notifiés au DPD, est un outil de planification précieux pour les institutions. Le CEPD recommande qu'un tel inventaire contienne au moins les champs suivants: nom du traitement, brève description du traitement (dont les finalités), notification au titre de l'article 25 (effectuée ou non), notification au titre de l'article 27 (requis et effectuée ou non) et personne de contact (responsable du traitement «dans la pratique».)*

<sup>8</sup> Le nombre moyen de traitements relevant de l'article 27 s'élève à 20 si l'on exclut la Commission, qui en comptabilise plus de 200.

institutions de maturité similaire s'agissant des fonctions de protection des données, résultant en quatre groupes (A à D)<sup>9</sup>.

Institution/organe	% de notifications au titre de l'article 25	% de notifications au titre de l'article 27	Taux article 25 par rapport à l'enquête de 2013	Taux article 27 par rapport à l'enquête de 2013
CCE	100%	90%	+/- 0	- 10
CE	97%	91%	+ 1	- 9
Conseil	98%	100%	+ 4	+/- 0
BCE	100%	83%	+/- 0	+/- 0
CJUE	95%	97%	- 2	+4
CDR	100%	100%	+ 2	+/- 0
CESE	93%	100%	- 6	+ 5
BEI	92%	84%	- 8	-13
PE	91%	92%	- 2	-8
OLAF	94%	100%	- 6	+/- 0
MEDIATEUR	81%	100%	- 19	+/- 0
CDT	72%	93%	- 3	+ 1
<b>Moyenne du groupe</b>	<b>96%</b>	<b>93%</b>	<b>-3</b>	<b>-3</b>

**Tableau 1: Taux de notification pour les institutions du groupe A**

Les institutions du groupe A affichent en moyenne des taux de notification assez élevés, la plupart dans des valeurs de 90 %. Ainsi que cela a été indiqué précédemment, le fait de partir d'un niveau si élevé limite les possibilités d'amélioration et plusieurs institutions ont enregistré des taux inférieurs par rapport à ceux indiqués dans l'enquête de 2013. Si ces fluctuations sont constatées à un niveau élevé, ce n'est pas nécessairement préoccupant. Cela souligne néanmoins que le registre est un document vivant: de nouveaux traitements sont ajoutés, d'anciens traitements sont parfois retirés, des traitements existants sont mis à jour. En réalité, plusieurs réponses font référence à des révisions du registre, ce qui se traduit souvent par une mise à jour des notifications. Cela signifie que le travail n'est pas terminé lorsqu'un registre est complété pour la première fois.

Cela étant dit, certaines des baisses sont perceptibles. La baisse des taux de notification au titre de l'article 27 à la BEI est due à l'identification de nouveaux traitements supplémentaires soumis à un contrôle préalable.

Le Médiateur a également identifié des traitements supplémentaires qui doivent être notifiés, ce qui se traduit par une baisse temporaire du taux de notification au titre de l'article 25.

Institution/organe	% de notifications au titre de l'article 25	% de notifications au titre de l'article 27	Taux article 25 par rapport à l'enquête de 2013	Taux article 27 par rapport à l'enquête de 2013
CEDEFOP	98%	100%	+ 8	+ 7

<sup>9</sup> Voir annexe 3 pour une explication de la manière dont les groupes ont été créés.



OCVV	87%	86%	- 4	- 4
EASME	100%	100%	+ 10	+ 10
AESA	94%	100%	+ 13	+ 35
CEPD	94%	100%	- 4	+/- 0
AEE	86%	100%	- 9	+/- 0
EFSA	94%	100%	+ 16	+ 16
FEI <sup>10</sup>	34%	47%	-	-
OEDT	74%	93%	- 2	+/- 0
EMA	96%	91%	- 4	- 3
AESM	100%	92%	+ 3	+ 7
ECSEL <sup>11</sup>	15% <sup>12</sup>	100%	-	-
ENISA	92%	100%	+ 3	+/- 0
ETF	100%	100%	+/- 0	+/- 0
EUROFOUND	100%	100%	+ 8	+/- 0
FRA	100%	100%	+ 4	+/- 0
OHMI	94%	97%	+ 4	+ 7
EU-OSHA	97%	100%	+ 1	+/- 0
<b>Moyenne du groupe</b>	<b>90 %</b>	<b>94 %</b>	<b>+3</b>	<b>+5</b>

**Tableau 2: Taux de notification pour les institutions du groupe B**

Les institutions du groupe B affichent dans l'ensemble de solides résultats, la FRA, Eurofound, l'EASME et l'ETF ayant enregistré des scores parfaits. Le CEDEFOP et l'EU-OSHA ont presque obtenu des scores parfaits, à une ou deux notifications près.

Il convient de mentionner tout particulièrement les résultats de l'AESA, qui figurait plutôt parmi les derniers dans son groupe de pairs. Ses faibles résultats dans l'enquête de 2011 ont conduit le CEPD à effectuer une visite de contrôle au printemps 2012; une amélioration considérable a pu être constatée dans l'enquête de 2013. Le rapport de cette enquête indiquait que l'AESA avait déjà fait beaucoup de progrès, mais que d'autres actions étaient attendues. L'AESA a obtenu des résultats et figure désormais parmi les bons élèves.

L'AEE a identifié plusieurs nouveaux traitements et a aussi subi une réorganisation, ce qui a nécessité certaines mises à jour; ces évolutions se sont traduites par une baisse temporaire.

Il n'est pas facile de comparer certains chiffres par rapport à ceux de la dernière enquête.

Le FEI s'appuie en partie sur la BEI pour de nombreux traitements administratifs. L'enquête de 2013 avait conclu que parmi les traitements indépendants du FEI, très peu avaient été notifiés et que la majorité des traitements inclus dans le registre étaient en réalité des notifications «du groupe BEI», pour lesquelles le FEI s'appuyait sur la BEI. Dans le même temps, le FEI a commencé une révision de son inventaire et de son registre, et a trouvé un nombre important de traitements supplémentaires (64 traitements identifiés dans l'inventaire, contre 23 traitements propres au FEI plus 16 traitements du groupe BEI). Les chiffres reflètent la situation à la date de la réponse du FEI à l'enquête - après la date limite, le FEI a fait beaucoup de progrès (voir aussi la section 3.3 ci-dessous). L'ECSEL résulte de la fusion

<sup>10</sup> Les chiffres du FEI ne peuvent être utilement comparés à ceux de l'enquête de 2013, voir ci-dessous.

<sup>11</sup> L'ECSEL résulte de la fusion des anciennes entreprises communes ARTEMIS et ENIAC, de sorte qu'il n'est pas facile de comparer les chiffres par rapport à ceux de la dernière enquête

<sup>12</sup> Voir explication p. 8 ci-dessous.

des anciennes entreprises communes ARTEMIS et ENIAC, de sorte qu'il n'est pas facile de comparer les chiffres par rapport à ceux de la dernière enquête. Si l'ECSEL a «hérité» de certaines procédures et traitements de ses prédécesseurs (comme ceux identifiés en vue d'un contrôle préalable), une révision complète de l'inventaire et du registre est en cours; selon les prévisions de l'ECSEL, toutes les notifications à jour ont dû être envoyées au DPD d'ici fin septembre.

Le taux de notification au titre de l'article 25 de l'OEDT est l'un des plus faibles dans ce groupe. Contrairement à plusieurs autres agences, cela semble réellement refléter une absence de progrès, étant donné que le nombre de notifications a stagné. L'OEDT devrait prendre des mesures pour combler cette lacune.

Institution/organe	% de notifications au titre de l'article 25	% de notifications au titre de l'article 27	Taux article 25 par rapport à l'enquête de 2013	Taux article 27 par rapport à l'enquête de 2013
EACEA	98%	96%	+/- 0	+ 1
CHAFEA	82%	100%	+ 30	+/- 0
ECDC	100%	100%	+ 4	+/- 0
AECP	96%	100%	+ 17	+/- 0
AFE	92%	93%	+ 6	+ 4
FRONTEX <sup>13</sup>	88%	90%	-	-
GSA <sup>14</sup>	52%	54%	-	-
INEA	91%	100%	+ 22	+ 37
Cleansky 2	100%	100%	+ 7	+/- 0
ECHA	100%	100%	+/- 0	+/- 0
ERCEA	90%	100%	- 8	+ 5
F4E	64%	73%	- 2	- 10
EC PCH	100%	100%	+/- 0	+ 33
IMI	75%	100%	- 25	+/- 0
REA	89%	93%	- 7	+ 11
SESAR	-	-	-	-
<b>Moyenne du groupe</b>	<b>88%</b>	<b>93%</b>	<b>+3</b>	<b>+6</b>

Tableau 3: Taux de notification pour les institutions du groupe C

Le groupe C n'est plus à la traîne derrière le groupe B, ce qui montre que si des efforts sont requis pour configurer l'inventaire et le registre, ce n'est pas impossible. L'ECHA, l'EC PCH, Cleansky et l'ECDC ont enregistré des scores parfaits; l'EACEA et l'AECP les suivent de très près.

En raison de certains points préoccupants, Frontex a reçu une visite de contrôle du CEPD fin 2012. Pour l'enquête de 2013, la visite ne semblait pas encore avoir produit beaucoup d'effets. Cette année, cependant, Frontex a affiché des résultats solides. La coopération avec Frontex s'est considérablement améliorée; Frontex s'est montrée particulièrement

<sup>13</sup> Frontex a seulement fourni une copie de son registre pour l'enquête de 2013, pas pour l'inventaire, de sorte qu'aucune comparaison utile n'a pu être établie.

<sup>14</sup> La GSA n'a pas répondu à l'enquête de 2013 dans les temps, de sorte qu'aucune comparaison utile n'a pu être établie.

coopérative lors d'une inspection réalisée en 2014 et a modifié ses activités en vue d'établir des traitements supplémentaires de données à caractère personnel à des fins opérationnelles.

Les taux de notification de F4E ont légèrement baissé. Cependant, les pourcentages masquent le fait que les chiffres absolus dans l'inventaire et le registre ont considérablement augmenté - pour l'article 25, de 21 sur 32 à 38 sur 59; pour l'article 27, de 15 sur 18 à 22 sur 30. Les chiffres ne reflètent donc pas une stagnation, mais plutôt une tendance à la hausse.

À la date limite, la GSA affichait toujours de moins bons résultats que ses pairs (voir aussi la section 3.4 ci-dessous) et la SESAR n'a pas répondu à l'enquête sur le fond (voir la section 2.6 ci-dessous).

Institution/organe	% de notifications au titre de l'article 25	% de notifications au titre de l'article 27	Taux article 25 par rapport à l'enquête de 2013	Taux article 27 par rapport à l'enquête de 2013
ACER	34%	36%	+ 6	+ 5
ORECE <sup>15</sup>	36%	31%	+ 23	- 2
CEPOL	24%	56%	+ 21	+ 13
EASO	54%	62%	+ 35	+ 37
ABE	100%	29%	+ 86	- 38
AED	100%	100%	-	-
SEAE	80%	47%	+ 48	- 20
EIGE	50%	86%	- 13	+/-0
AEAPP	13%	44%	+/-0	- 14
EIT	28%	38%	+ 13	- 32
AEMF	32%	29%	- 3	- 32
CERS <sup>16</sup>	voir BCE	voir BCE	-	-
IESUE	25%	17%	+ 25	+ 17
eu-LISA	81%	11%	+ 81	+ 11
CSUE	52%	100%	+ 52	+ 100
<b>Moyenne du groupe</b>	<b>53%</b>	<b>47%</b>	<b>+29</b>	<b>+3</b>

Tableau 4: Taux de notification pour les institutions du groupe D

Le groupe D est composé des organes et des agences les plus récents; les taux de notification sont donc souvent plus faibles. Étant donné qu'il n'est pas rare que ces agences n'aient pas encore fini d'établir leurs processus opérationnels, leurs inventaires ont tendance à être moins établis aussi.

L'ACER en est un exemple: alors que son taux de notification au titre de l'article 25 n'a que légèrement augmenté, cela masque le fait que le nombre de notifications dans le registre a

<sup>15</sup> L'ORECE a notifié plusieurs traitements supplémentaires relevant de l'article 27 après la date limite de dépôt des contributions à l'enquête, de sorte qu'ils n'ont pas pu être pris en considération pour le présent calcul.

<sup>16</sup> Les traitements du CERS sont intégrés dans la documentation de la BCE; le DPD de la BCE est aussi le DPD du CERS.

presque triplé - cette hausse est atténuée par une augmentation similaire du nombre de traitements identifiés dans l'inventaire<sup>17</sup>.

De même, l'augmentation du nombre de notifications au titre de l'article 25 au SEAE est en réalité plus importante que ne le suggèrent les pourcentages de notification. Alors qu'en 2013, il avait identifié 65 traitements dans son inventaire, ce chiffre est passé à 118 en 2015; ses efforts pour augmenter le taux de notification se sont donc avérés payants. La baisse des notifications au titre de l'article 27 est le résultat d'efforts similaires: sur 32 traitements, 15 sont enregistrés comme notifiés, par rapport à 10 sur 15 en 2013, ce qui se traduit par un taux plus faible, mais représente néanmoins un meilleur contrôle de ses traitements.

L'ABE semble avoir porté son attention en premier sur les notifications au titre de l'article 25, ce qui montre une amélioration impressionnante, surtout compte tenu de la croissance de l'inventaire, dont le nombre d'entrées est passé de 35 à 58. L'identification de nouveaux traitements a aussi révélé un plus grand nombre de dossiers relevant de l'article 27, ce qui s'est traduit par une baisse significative du taux de notification au titre de l'article 27 (de 4 sur 6 à 5 sur 17). La prochaine étape pour l'ABE consistera donc à combler cette lacune.

L'EASO est un exemple d'agence qui améliore constamment ses résultats; alors qu'elle se trouvait en dessous de la moyenne dans son groupe, elle passe légèrement au-dessus.

L'EIT enregistre des améliorations en ce qui concerne l'article 25, mais le taux de notification au titre de l'article 27 a baissé en raison de l'identification de traitements supplémentaires qui doivent être notifiés.

eu-LISA, dont le DPD permanent n'a été désigné qu'au printemps 2014, a enregistré d'excellents progrès en ce qui concerne les notifications au titre de l'article 25, alors qu'elle était partie de zéro dans l'enquête de 2013. Cependant, elle est à la traîne en ce qui concerne les notifications au titre de l'article 27 et elle devrait prendre des mesures pour combler cette lacune.

Plusieurs des agences de ce groupe qui avaient montré un démarrage lent dans les enquêtes précédentes ont reçu les visites ou des détachements de personnel du CEPD entre-temps, dans le but d'améliorer la conformité:

Le CSUE a bénéficié d'un détachement de personnel du CEPD à l'automne 2014 et a effectivement rattrapé son retard en ce qui concerne les notifications au titre de l'article 25; sur l'article 25, il se dirige dans la bonne direction.

L'EIGE avait déjà été épinglé pour une visite à la suite de l'enquête de 2011, laquelle a été effectuée au printemps 2013. L'enquête de 2013 avait déjà montré des résultats, avec des scores respectables pour une agence de son âge. Cependant, l'EIGE semble avoir perdu de son élan et ne devrait pas se reposer sur ses lauriers, mais continuer d'améliorer sa conformité.

L'AEAPP connaît la même tendance à la hausse que l'ACER et le SEAE: le nombre d'entrées dans l'inventaire a presque doublé entre 2013 et 2015 (70 au lieu de 40). La baisse des taux de notification au titre de l'article 27 est due au fait que plusieurs traitements futurs ont déjà été identifiés en vue d'un contrôle préalable dans l'inventaire.

L'IESUE a désigné son premier DPD à la suite de l'enquête de 2013. À l'automne 2014, une visite de consultation a eu lieu au niveau du personnel. Malgré les progrès réalisés, l'IESUE

---

<sup>17</sup> En 2013, l'ACER a enregistré 9 notifications effectuées sur 32 au titre de l'article 25; cette fois, sur 92, elle a enregistré 31 notifications effectuées.

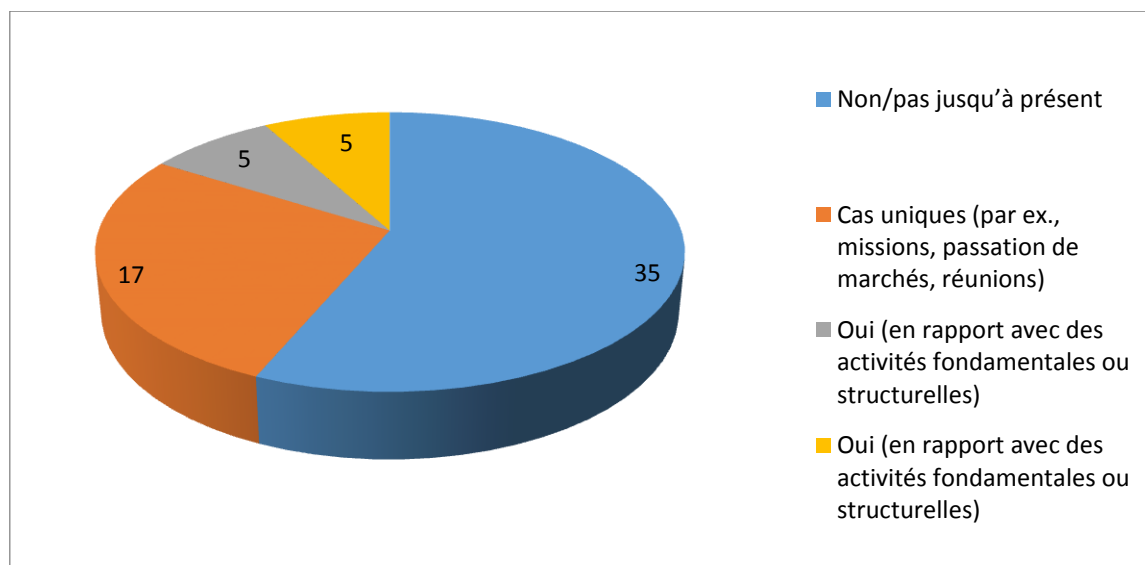
devrait accroître ses activités de conformité. Cela nécessite notamment des unités opérationnelles qu'elles fournissent au DPD leurs notifications au titre de l'article 25, de sorte que la procédure de contrôle préalable puisse être lancée en cas de besoin.

Le directeur exécutif de l'AEMF et le CEPD se sont rencontrés au printemps 2013; en été 2015, une visite de consultation a été organisée. La baisse significative du taux de notification au titre de l'article 27 est due à l'identification de nombreux traitements additionnels qui relèvent de cet article.

## 2.2. Transferts en 2013-2014 à des destinataires non soumis aux dispositions nationales adoptées en application de la directive 95/46/CE

**Ça vous dit quelque chose?** Déjà lors de l'exercice de 2013 (enquête 2013)<sup>18</sup>, le CEPD avait demandé aux institutions de l'UE de fournir des informations sur les transferts de données à caractère personnel à des destinataires non soumis à la législation nationale adoptée en application de la directive 95/46/CE. Le CEPD avait ensuite demandé des informations sur ces transferts sous la forme d'une question ouverte afin d'obtenir une vue générale et également d'élaborer des orientations.

En 2013, sur un total de 62 institutions et organes de l'UE, 35 entités ont déclaré n'avoir effectué aucun transfert de ce type; 17 autres institutions ont affirmé qu'il n'y avait pas de transferts structurels, mais qu'ils pouvaient se présenter dans des cas spécifiques exceptionnels. Dans ce contexte, le CEPD avait donc conclu (enquête 2013, p. 18) que: «**Les transferts relevant de l'article 9 dans le cadre des activités fondamentales des institutions de l'UE sont rares**».



Graphique 1: Aperçu des transferts relevant de l'article 9 (exercice 2013)

**Qu'est-ce qui a changé?** En juillet 2014, le CEPD a publié un document d'orientation sur «Le transfert de données à caractère personnel à des pays tiers et à des organisations

<sup>18</sup> Voir [https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Inquiries/2014/14-01-24\\_survey\\_report\\_FR.pdf](https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Inquiries/2014/14-01-24_survey_report_FR.pdf).

internationales par les institutions et organes de l'Union européenne»<sup>19</sup>. Dans ce contexte, pour le **présent exercice**, le CEPD s'est renseigné sur les récents transferts de données à caractère personnel relevant de l'article 9 au cours des années 2013 et/ou 2014. Sur un total de 61 institutions, 18 seulement ont répondu par l'affirmative. Par conséquent, les transferts relevant de l'article 9 dans le cadre des activités fondamentales des institutions de l'UE restent rares<sup>20</sup>. Cependant, étant donné que ces transferts sont associés à des **risques accrus**, nous avons invité les institutions concernées à fournir des **informations plus détaillées** dans le cadre du présent exercice.

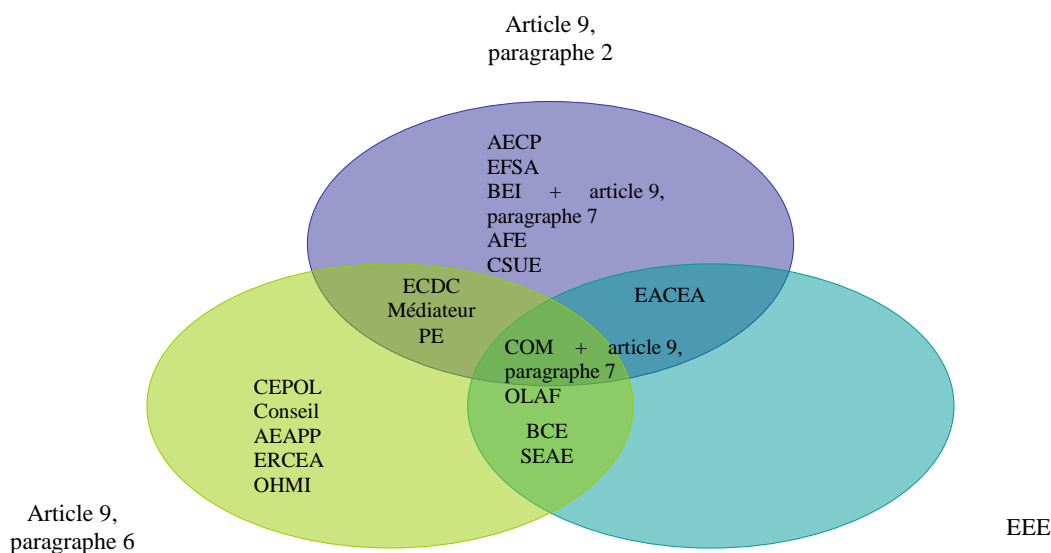
---

<sup>19</sup>[https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Papers/14-07-14\\_transfer\\_third\\_countries\\_FR.pdf](https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Papers/14-07-14_transfer_third_countries_FR.pdf).

<sup>20</sup> La baisse par rapport à l'exercice de 2013 peut s'expliquer par la limitation à une période spécifique (par exemple, la CJUE a indiqué que certains traitements en principe prévoient de tels transferts, mais que ces transferts n'ont pas eu lieu en 2013 ni en 2014). D'autres institutions ont indiqué qu'elles ne considéraient pas certains transferts relevant de l'article 9 comme les *leurs* (par exemple, le CEPD pour ceux réalisés par des prestataires tiers pour leurs propres finalités ou le Cedefop pour le personnel qui communique ses données à caractère personnel à des organisateurs de réunions/conférences/événements dans des pays tiers).

**Les différents types de transferts relevant de l'article 9:** Lorsque des transferts avaient été réalisés au cours de cette période, les institutions de l'UE ont été invitées à indiquer séparément les transferts relevant de l'article 9, paragraphe 2 (appréciation du caractère adéquat), de l'article 9, paragraphe 6, ou de l'article 9, paragraphe 7 (dérogations) et les transferts relevant de l'article 9 aux destinataires qui sont établis dans des pays de l'EEE, mais qui réalisent des types d'activités qui sont exclus de l'application de la directive 95/46/CE (par exemple, aux autorités judiciaires).

**L'article 9 du règlement** concerne essentiellement les transferts à des pays tiers et à des organisations internationales. Dans la mesure où les transferts à des tiers impliquent nécessairement une certaine perte de contrôle sur des données à caractère personnel, il est important que les destinataires soient soumis à des règles strictes en matière de protection des données. Ce n'est pas un problème pour les transferts au sein des institutions de l'UE ou entre des institutions de l'UE, ni pour les transferts à la plupart des destinataires dans l'UE. Pour les transferts à d'autres tiers, cela peut devenir un problème puisque leurs normes en matière de protection des données sont souvent plus faibles que la norme européenne. C'est la raison pour laquelle l'article 9, qui régit ces transferts, est plus restrictif que les règles applicables aux transferts intra-UE. Cela reflète le **risque accru qui les caractérise.**



**Graphique 2: Diagramme des types de transferts relevant de l'article 9 (exercice 2015)**

Sur les 18 institutions<sup>21</sup> qui ont enregistré des transferts relevant de l'article 9 au cours de cette période, trois (l'EFSA, la CJUE et le Médiateur) ont explicitement mis en avant

<sup>21</sup> La Commission a fourni des informations plus détaillées: sur les 41 Directions générales, 14 avaient réalisé des transferts relevant de l'article 9 au cours de cette période. L'AESM a indiqué que «Les seules données que l'AESM serait susceptible de transférer, à des acteurs en dehors de l'UE, généralement avec une intermédiation de l'agence de voyage, seraient des données limitées utilisées pour des services de réservation de voyages dans le cadre de missions du personnel de l'AESM: transport et hôtels. La réalité ne justifie pas d'appliquer l'article 9».

**l'utilisation des médias sociaux:** Twitter<sup>22</sup>, YouTube, LinkedIn et Flickr (EFSA) mais aussi Google+ (Médiateur).

- Des indications supplémentaires concernant les transferts relevant de l'article 9 ont été demandées dans un tableau concernant l'activité de traitement (telle que mentionnée dans la notification au titre de l'article 25), le destinataire, la base (par exemple, appréciation du caractère adéquat par le responsable du traitement), le domaine (par exemple, application de la loi), le «comment» du transfert (par exemple, en envoyant les données par la poste, par courrier électronique, en accordant l'accès à une base de données, etc.), les catégories de données à caractère personnel ainsi que la fréquence de ces transferts.
- En outre, le CEPD souhaitait savoir si les agences avaient rencontré des difficultés particulières dans les activités ci-dessus et, si possible, les raisons de ces difficultés.
- Enfin, le CEPD souhaitait savoir s'il existait un système interne de suivi et d'enregistrement des transferts relevant de l'article 9.

En ce qui concerne les **transferts relevant de l'article 9, paragraphe 2**, 11 institutions<sup>23</sup> ont effectué des transferts en 2013 et/ou 2014 concernant des catégories très différentes de données à caractère personnel dans plusieurs domaines et à une fréquence variable (ces éléments ne sembleraient pas permettre de tirer d'autres conclusions en plus du traitement individuel). Par exemple, l'EACEA a effectué ces transferts aux fins d'octroyer et de mettre en œuvre des subventions dans le domaine de l'éducation, l'AECP dans le contexte de la transmission de rapports d'inspection concernant des bateaux de pêche, la BEI pour le calcul actuariel de droits à pension du personnel (également pour la gestion des pensions: CSUE).

Les destinataires comprennent des organisations internationales (par exemple, l'OCDE pour la BEI, l'OMS, la FAO et l'OCDE pour l'EFSA), mais aussi des autorités régionales et nationales et des points de contact désignés (par exemple, pour la DG EAC et l'EACEA pour les programmes éducatifs/professionnels, autorités chargées des transports dans le cas de l'AFE ou autorités douanières pour la DG TAXUD).

Dans la majorité des cas, le transfert repose sur une appréciation du caractère adéquat réalisée par le responsable du traitement (par exemple, la DG AGRI pour le contrôle des informations sur l'agriculture biologique). D'autres possibilités comprennent, par exemple, une décision d'adéquation prise par la Commission européenne (par exemple, la DG RTD pour l'évaluation des propositions et la gestion des subventions) ou l'accord sur la sphère de sécurité entre l'UE et les États-Unis.

12 institutions<sup>24</sup> ont enregistré des **transferts relevant de l'article 9, paragraphe 6** en 2013 et/ou 2014, là encore concernant des catégories très différentes de données à caractère personnel dans plusieurs domaines.

---

<sup>22</sup> Voir [https://secure.edps.europa.eu/EDPSWEB/edps/cache/off/EDPS/Legal\\_notice/Twitter\\_policy](https://secure.edps.europa.eu/EDPSWEB/edps/cache/off/EDPS/Legal_notice/Twitter_policy) pour la politique Twitter du CEPD. Des orientations supplémentaires devraient être disponibles d'ici la publication des directives de communications électroniques du CEPD.

<sup>23</sup> La Commission a indiqué que sur les 41 directions générales, 7 ont effectué des transferts relevant de l'article 9, paragraphe 2, au cours de cette période.

<sup>24</sup> La Commission a indiqué que sur les 41 directions générales, 9 ont effectué des transferts relevant de l'article 9, paragraphe 6, au cours de cette période.



Les principaux destinataires comprennent des agences de voyage (CEPOL, BCE, AEAPP<sup>25</sup>); des agences de gestion des visas/consulats (BCE, AEAPP); diverses organisations régionales et internationales (par exemple, dans le domaine de la gestion des pêches pour la DG MARE ou l'OMS pour la DG SANTE et l'ECDC) et les autorités douanières pour la DG TAXUD.

Presque toutes les possibilités offertes par l'article 9, paragraphe 6, ont été mentionnées comme base juridique dans les réponses des institutions:

- l'article 9, paragraphe 6, point a), est invoqué par la DG ESTAT pour enregistrer les participants à un concours vidéo et par la DG TAXUD pour accéder à un espace collaboratif dans le cadre de la participation aux programmes Fiscalis et Douane;
- l'article 9, paragraphe 6, point c), est cité en ce qui concerne la gestion d'agents locaux dans les délégations de l'UE et pour des transferts effectués par le SEAE concernant la sécurité sociale et l'administration fiscale;
- l'article 9, paragraphe 6, point d), est la base utilisée par la DG MARE dans le cadre de la notification des navires et par la DG JUST dans le cadre de son système d'alerte rapide concernant les produits dangereux non alimentaires;
- les points d) et e), de l'article 9, paragraphe 6, sont utilisés par le Conseil pour des missions dans des pays tiers et par la DG SANTE pour son système d'alerte précoce et de réaction.

**Les transferts relevant de l'article 9, paragraphe 7** sont effectués vers des destinataires n'assurant pas un niveau de protection adéquat, mais pour lesquels le responsable du traitement offre des garanties suffisantes<sup>26</sup>. Ces transferts sont rares: seulement deux DG de la Commission (DG SANTE et DG TAXUD) et la BEI ont identifié de tels transferts (même si aucun n'a encore été effectué pour la BEI).

Quatre institutions seulement (EACEA, BCE, SEAE et OLAF) ont noté qu'elles avaient transféré des données à caractère personnel relevant de l'article 9 à des destinataires qui sont établis dans des **pays de l'EEE**, mais qui réalisent des types d'activités qui sont exclus de l'application de la directive 95/46/CE (par exemple, à la police ou à des autorités judiciaires<sup>27</sup>).

\*\*\*

***Une absence totale de problèmes?*** Compte tenu de la fréquence et parfois de la complexité des activités susmentionnées, il est surprenant que la BEI ait été la seule à avoir indiqué **rencontrer des difficultés**, précisant qu'il était difficile d'établir **l'adéquation de pays tiers**. En effet, le CEPD a reconnu dans son document d'orientation (p. 13, section 5.2) que «...dans la pratique, il ne lui est pas toujours possible de réaliser une appréciation complète de l'adéquation pour un pays tiers ou une organisation internationale. Le cas échéant, le

---

<sup>25</sup> L'AESM a indiqué que «Les seules données que l'AESM serait susceptible de transférer, à des acteurs en dehors de l'UE, généralement avec une intermédiation de l'agence de voyage, seraient des données limitées utilisées pour des services de réservation de voyages dans le cadre de missions du personnel de l'AESM: transport et hôtels. La réalité ne justifie pas d'appliquer l'article 9».

<sup>26</sup> Voir document d'orientation p. 14, section 6. Voir document d'orientation pp. 21/22, section 6.3 concernant l'association obligatoire du DPD à la procédure d'analyse conduite avant l'adoption de mesures adéquates ainsi que les trois scénarios qui doivent être pris en considération pour l'association du CEPD ex-ante.

<sup>27</sup> Voir document d'orientation, pp. 22/23, section 7. Ainsi qu'il est indiqué dans ce document: «Ces exceptions étaient nécessaires avant l'adoption du traité de Lisbonne, mais elles sont désormais, en principe, incompatibles avec son article 16, ainsi qu'avec l'article 8 de la charte des droits fondamentaux de l'Union européenne».

responsable du traitement devrait présumer que le niveau de protection n'est pas adéquat et **envisager d'autres options...**».

Lorsque le responsable du traitement décide néanmoins de réaliser **une appréciation de l'adéquation**<sup>28</sup>, le CEPD a noté dans le document d'orientation (pp. 13+14, sections 5.2 et 5.3) que «à la lumière du principe de responsabilité, le responsable du traitement des données devrait, le cas échéant, **documenter de manière exhaustive les mesures prises pour veiller à l'adéquation**, et envisager d'effectuer une évaluation des risques appropriée.» En outre, «Toute analyse effectuée par le responsable du traitement devrait être...mise à disposition du CEPD à sa demande».

Ainsi que cela est également noté dans le document d'orientation du CEPD (p. 14, section 5.3), «Au regard de la politique relative aux consultations dans le domaine de la supervision et de la mise en application, le **DPD** d'une institution ou d'un organe de l'Union devrait toujours être consulté et associé à l'analyse. Par ailleurs, les responsables du traitement des données sont encouragés à solliciter un avis du **CEPD** lorsque l'affaire: a) présente une nature ou une complexité inédites (lorsque le DPD ou l'institution ont des doutes importants), ou b) qu'elle a une incidence claire sur les droits des personnes concernées (en raison notamment des risques liés aux opérations de traitement, etc.)».

\*\*\*

En ce qui concerne l'existence d'un **système interne de suivi et d'enregistrement** des transferts relevant de l'article 9, six institutions seulement ont signalé l'existence d'un tel système. Une institution a annoncé qu'un tel système serait bientôt mis en place, tandis qu'une autre institution importante envisage de centraliser son(ses) système(s) existant(s).

Le CEPD constate avec préoccupation qu'environ un quart seulement de toutes les institutions effectuant des transferts relevant de l'article 9 dispose d'un système interne de contrôle et d'enregistrement. Dans le document d'orientation (p. 9, section 3.4), le CEPD a noté qu'un tel système serait «utile pour contribuer à la gestion interne des transferts internationaux et veiller à une responsabilisation et à une conformité effectives dans le cadre du règlement». Le CEPD avait donc recommandé la création de ces systèmes dans le cadre des bonnes pratiques, soulignant que «Celui-ci devrait non seulement inclure les transferts sur la base de leur caractère adéquat, mais aussi, et surtout, les transferts reposant sur des dérogations (article 9, paragraphes 6 et 7)».

Pour **veiller à une responsabilisation et à une conformité effectives dans le cadre du règlement**, le CEPD recommande donc aux institutions de mettre en place un système interne d'enregistrement des transferts relevant de l'article 9.

**Graphique 3: Aperçu des réponses sur les transferts (exercice 2015)**

<i>T1</i> Transferts relevant de l'article 9		<i>T2</i> Article 9, paragraphe 2	<i>T3</i> Article 9, paragraphe 6	<i>T4</i> Article 9, paragraphe 7	<i>T5</i> EEE	<i>T7</i> Système de suivi/d'enregistrement
CEPOL COM (par DG <sup>29</sup> )		COM (7 DG)	CEPOL COM (9 DG) Conseil	COM (2 DG)		COM (2 DG)

<sup>28</sup> Voir pp. 10 - 12, section 4.2 du document d'orientation sur la notion «d'adéquation».

<sup>29</sup> AGRI, EAC, GROW, HR, MARE, RTD, TAXUD pour l'article 9, paragraphe 2; EMPL, ESTAT, JUST, MARE, NEAR, PMO, SANTE, TAXUD, TRADE pour l'article 9, paragraphe 6.

Conseil EACEA BCE ECDC SEAE AACP EFSA BEI AEAPP PE AFE ERCEA CSUE OHMI OLAF Médiateur		EACEA  ECDC  AACP EFSA BEI  PE AFE  CSUE  OLAF Médiateur	BCE ECDC SEAE   AEAPP PE  ERCEA  OHMI OLAF Médiateur	BEI	EACEA BCE  SEAE      OLAF	ECDC  AACP  BEI («bientôt») AEAPP  ERCEA  OLAF
18		11	12	2	4	6

**Le «comment» du transfert.** La plupart des transferts sont effectués par trois voies de communication principales: par courrier (lettre, parfois recommandée, ou «note verbale»; 8 cas), par courrier électronique (parfois crypté; 11 cas) ou en accordant l'accès à une base de données particulière (7 cas) ou par une association de ces voies (5 cas). D'autres possibilités comprennent les transferts par télécopie, un formulaire en ligne, par téléphone ou remise en main propre.

### 2.3. Sécurité de l'information

Le CEPD a posé les questions suivantes:

- existe-t-il un processus spécialement dédié à la gestion de la sécurité de l'information?
- les traitements sont-ils soumis à une évaluation des risques? Le cas échéant, le CEPD a demandé d'indiquer la proportion (%) des traitements qui ont été soumis à une évaluation des risques au cours des deux dernières années.
- l'institution a-t-elle mis en place une politique de sécurité générale<sup>30</sup>? Le cas échéant, la politique de sécurité générale comprend-elle une section sur la sécurité de l'information?
- un processus formel a-t-il été mis en place pour faire face aux incidents de sécurité?
- le DPD reçoit-il une notification si l'incident de sécurité de l'information implique des données à caractère personnel?

<sup>30</sup> Cette question ne concernait pas des politiques de sécurité spécifiques à l'application.

Toutes les institutions, sauf huit, ont répondu qu'elles avaient mis en place un processus spécialement dédié à la gestion de la sécurité de l'information. Deux institutions prévoient d'établir un tel processus plus tard en 2015. Deux institutions ont explicitement mentionné la certification ISO (ECHA / ISO 9001) ou la mise en œuvre (GSA (GNSS); ISO 27001) dans ce contexte.

19 institutions ont répondu qu'elles ne soumettent pas leurs traitements à une évaluation des risques, du moins pas régulièrement, et une institution a noté qu'une telle approche n'était «pas réaliste dans une institution disposant de ressources limitées».

Une majorité d'institutions (38), cependant, ont explicitement confirmé qu'elles soumettaient leurs traitements de données à une évaluation des risques. Sur cette majorité, 18 institutions ont fourni des indications sur le pourcentage de traitements concernés par un tel exercice, allant de «négligeable» à 100 % (ce dernier pourcentage concernait huit institutions), ce qui signifie que, pour les institutions qui procèdent à une appréciation des risques et qui fournissent des pourcentages, en moyenne, deux-tiers (66,4 %) de leurs traitements ont été soumis à une appréciation des risques.

16 institutions ont indiqué qu'elles n'avaient pas de politique de sécurité générale, deux institutions ont fait part de leur intention d'en mettre une en place plus tard en 2015. Pour la plupart, ces politiques de sécurité générale comprennent une section sur la sécurité de l'information. Une institution a fait observer qu'elle n'avait pas de politique de sécurité générale mais une politique de sécurité des TIC.

45 institutions ont confirmé l'existence d'un processus formel pour faire face aux incidents de sécurité (13 ont clairement indiqué l'absence d'un tel processus), deux autres ont noté qu'un tel processus était en cours de développement.

REA: «...un outil en ligne est mis à la disposition de l'ensemble de la communauté de chercheurs et en cas de violation de la sécurité impliquant des données à caractère personnel...le responsable du traitement concerné devra utiliser ce formulaire pour signaler une violation de données...»

Six institutions seulement ont indiqué que leur DPD n'est pas averti lorsque l'incident de sécurité de l'information implique des données à caractère personnel<sup>31</sup>; une a noté l'absence d'une telle notification malgré les recommandations d'audit répétées à cet égard. Pour une institution, la notification a été identifiée comme étant liée aux tâches essentielles du DPD en tant que responsable informatique, plutôt qu'en sa qualité de DPD. Plusieurs institutions ont souligné la nature hypothétique d'une telle notification au DPD, étant donné qu'aucun incident de la sorte ne s'est produit.

Médiateur: «Bien qu'il n'existe pas de procédure standard de notification d'une violation de données à caractère personnel, par le passé, lorsqu'un incident de sécurité des données s'est produit, le DPD en a été officiellement informé. Notamment, le responsable de la protection des données a soumis un rapport de l'incident au DPD. Le

*En vertu de l'article 22, paragraphe 1, du règlement, compte tenu de l'état de l'art et des coûts liés à leur mise en œuvre, 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 sont prises notamment afin d'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.*

<sup>31</sup> Pour une institution, une telle obligation de notification sera incluse dans un processus formel, actuellement en cours de développement.

rapport contenait les informations suivantes: a) une chronologie des événements ayant conduit au transfert non autorisé des données à caractère personnel; b) le volume et la nature des données à caractère personnel qui ont été transférées et le nombre de personnes concernées; c) les mesures prises pour atténuer les éventuels effets négatifs de la violation des données à caractère personnel; d) les mesures prises pour informer les personnes concernées par l'incident ou les raisons pour lesquelles la décision a été prise de ne pas les informer; et e) les mesures prises pour empêcher qu'un tel incident ne se reproduise à l'avenir.»

Dans l'ensemble, les institutions de l'UE ont reconnu qu'il convient de gérer la sécurité de l'information comme un processus, à savoir que la sécurité de l'information n'est pas une question qui est réglée une fois pour toutes mais qui doit être constamment contrôlée et réévaluée. Cependant, il semble que les évaluations des risques n'aient pas totalement intégré les processus de sécurité de l'information des institutions de l'UE (les évaluations des risques sont un outil important lorsqu'il s'agit de dissiper les doutes concernant la gestion de la sécurité au sein d'une organisation<sup>32</sup>). Cela soulève la question de savoir comment les institutions de l'UE décident d'allouer les ressources et de déployer les efforts liés pour améliorer leur sécurité de l'information.

En outre, les incidents de sécurité<sup>33</sup> semblent être le plus souvent gérés officiellement au sein des institutions de l'UE, le DPD étant souvent associé lorsque des données à caractère personnel sont concernées. Cette approche garantit un traitement approprié des violations de données à caractère personnel, compte tenu de l'impact potentiel des violations de données pour les personnes concernées.

#### **2.4. Garantir l'effacement effectif des données à caractère personnel**

Le CEPD s'est renseigné sur l'existence:

- d'une **politique écrite** régissant l'effacement effectif des données à caractère personnel à la fin du délai de conservation;
- d'une **procédure standard** régissant l'effacement effectif des données à caractère personnel à la fin du délai de conservation;
- **de processus automatisés** soutenant la procédure d'effacement dans tous les systèmes;
- de mesures destinées à garantir **l'effacement** des informations **dans les copies de sauvegarde**, le cas échéant?

Sur 61 institutions, 38 ont indiqué avoir une **politique écrite régissant l'effacement effectif** des données à caractère personnel. Une institution a signalé qu'elle était en voie d'établir une telle politique. Cependant, certaines explications indiqueraient qu'une interprétation assez large de la «politique» sous-tend cette autoévaluation: un certain nombre d'institutions considéreraient qu'elles disposent d'une politique écrite lorsqu'un délai de conservation est fixé «par traitement» dans le registre du DPD. Deux institutions ont identifié

*L'article 4, paragraphe 1, point e), du règlement dispose que 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. En vertu de l'article 4, paragraphe 2, du règlement, il incombe au responsable du traitement d'assurer le respect du paragraphe 1.*

<sup>32</sup> Voir ISO 27001, ISO 27005, norme BSI 100-3, publication spéciale NIST 800-300, EBIOS, Octave Allegro, MAGERIT.

<sup>33</sup> Voir ISO 27035, NIST 800-61r2.

la mise en place d'une politique écrite comme un projet «futur» ou «en cours»; pour une institution, cette politique est actuellement «en attente d'approbation».

Le CEPD avait demandé une brève description de la politique générale, ou, si la politique est spécifique à chaque traitement ou à des traitements en particulier, une **description** précise. La plupart des institutions ont répondu en citant des exemples de traitements spécifiques, par exemple:

AECP: «En ce qui concerne les traitements dans le domaine des RH,...les archives des RH ont été structurées en huit sous-catégories de fichiers contenant des données à caractère personnel. La politique générale concernant le délai de conservation est exposée dans les notifications contenues dans le registre de la protection des données de l'AECP. Par conséquent, un tableau récapitulatif des délais de conservation des fichiers des RH a été extrait. Dans la feuille de route des RH, une révision et un suivi annuels des activités des RH sont inclus. Il en résulte un contrôle des archives et des délais de conservation et le lancement d'un exercice de destruction une fois par an».

IESUE: «Les règles relatives aux stages prévoient qu'à la fin du programme de stage, seul un volume de données limité (nom, prénom) sera conservé par l'agent chargé de la documentation et de la recherche ainsi qu'un rapport concernant les activités du stagiaire à des fins d'archivage et d'enregistrement (par exemple, lettres de références).»

En ce qui concerne l'existence d'une **procédure standard** régissant l'effacement effectif des données à caractère personnel à la fin du délai de conservation, 26 institutions ont répondu avoir une telle procédure en place. Deux autres ont indiqué que la création d'une telle procédure standard était un projet «futur» ou «en cours». Une institution a indiqué qu'une telle procédure standard existe «pour certains traitements uniquement».

ECHA: «L'ECHA a adopté une procédure de contrôle des documents et des registres... Elle fixe les principes de haut niveau concernant la conservation des documents. Les délais de conservation détaillés de tous les registres identifiés dans l'Agence sont mentionnés dans un autre document officiel, le calendrier de conservation des registres de l'ECHA. L'annexe à la procédure de contrôle des documents et registres donne des instructions détaillées et pratiques sur la manière dont les documents papier et électroniques doivent être détruits après l'expiration de leur délai de conservation.»

Seules 11 institutions affirment disposer de **processus automatisés soutenant la procédure d'effacement** dans tous les systèmes en place (11 institutions n'ont pas de systèmes respectifs et ont donc répondu «non disponible»). Cinq autres institutions ont indiqué que la création de tels processus automatisés était un projet «futur» ou «en cours». Les exemples donnés concernent souvent des séquences de vidéo surveillance (cinq institutions).

En ce qui concerne **l'effacement des informations dans les copies de sauvegarde**, 42 institutions ont indiqué faire en sorte d'effacer les copies de sauvegarde, mais la plupart n'ont décrit que brièvement, voire pas du tout, *comment* elles s'y prennent.

## 2.5. [Votre délégué à la protection des données et vous](#)

**Ça vous dit quelque chose?** Dans l'enquête de 2013, nous avons demandé des informations sur la manière dont les DPD participent à la conception de nouveaux traitements impliquant des données à caractère personnel, en mentionnant des documents d'administration (surtout dans le domaine informatique) le cas échéant, ou simplement en décrivant les bonnes pratiques en place, qu'elles soient formalisées ou non.

Cette question ayant été intentionnellement libellée de manière très ouverte, la forme des réponses variait fortement, mais il était tout à fait évident que nombre d'institutions de l'UE sont conscientes de la nécessité de réfléchir à la protection des données dès le départ et d'impliquer leur DPD. Nous en avons donc conclu que la manière de garantir cela diffère d'une institution de l'UE à l'autre.

**Qu'est-ce qui a changé?** Pour la présente édition 2015 de l'enquête, compte tenu des résultats précédents, le CEPD a posé des questions plus ciblées. Dans une section séparée, pour laquelle le CEPD a explicitement demandé que ce ne soit pas le DPD qui fournisse les réponses, le CEPD a demandé des informations pour savoir si les tâches du DPD font partie de la description de son poste, si l'exécution des tâches du DPD fait partie de l'évaluation de ses performances et comment le DPD participe à la conception de nouveaux traitements.

Ainsi que nous l'avons souligné dans la stratégie du CEPD<sup>34</sup>, nous comptons sur une étroite coopération avec les DPD pour soutenir les institutions de l'UE afin qu'elles s'orientent vers une approche non plus fondée exclusivement sur la conformité mais sur la responsabilisation.

**La participation du DPD:** Dans l'enquête de 2013, plusieurs institutions avaient mentionné dans leurs réponses que les DPD n'étaient pas impliqués suffisamment (tôt) ou que les consultations étaient trop générales. Dans leurs réponses pour l'édition 2015, toutes les institutions affirment que le DPD participe à la conception de nouveaux traitements, même si la plupart des institutions n'ont pas réellement décrit comment leur DPD participe, mais ont simplement répondu par l'affirmative<sup>35</sup>. Deux institutions ont tout particulièrement signalé une participation accrue de leur DPD. Plusieurs institutions, cependant, ont fait part de réserves graduelles indiquant «est susceptible d'être consulté», «de temps en temps», «le cas échéant», «si besoin est» ou «en temps que de besoin/sur une base ad hoc/au cas par cas».

*On ne soulignera jamais assez l'importance du délégué à la protection des données (DPD) en tant que partenaire des responsables du traitement des institutions de l'UE ainsi que du CEPD. Le DPD joue un rôle crucial dans le respect du règlement. Il est le premier point de contact vers lequel se tourne le personnel des institutions de l'UE pour obtenir des conseils sur ses droits et obligations et il œuvre au renforcement de la culture en matière de protection des données. En outre, il est le principal interlocuteur du CEPD. En interne, les DPD peuvent diffuser des bonnes pratiques au sein de leur institution respective, jouer le rôle de pôle de connaissances, fournir des conseils aux responsables du traitement et signaler des problèmes. Le fait d'associer les DPD à un stade précoce de la conception de nouveaux traitements est une bonne façon de garantir le respect de la vie privée dès la conception.*

<sup>34</sup> [https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Strategy/15-07-30\\_Strategy\\_2015\\_2019\\_Update\\_FR.pdf](https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Strategy/15-07-30_Strategy_2015_2019_Update_FR.pdf), p. 20.

<sup>35</sup> Par exemple, le CSUE a indiqué que «tous les traitements doivent être soumis au contrôle du DPD en vue d'établir leur conformité»

Conseil: «En ce qui concerne les traitements qui ne comprennent pas le développement de nouveaux systèmes informatiques, le DPD est généralement consulté à un stade précoce pour s'assurer que les traitements envisagés respectent les exigences en matière de protection des données. Les questions qui sont le plus souvent soulevées sont les suivantes: qualité des données, destinataires, mesures de sécurité, délais de conservation des données et information des personnes concernées.

Dans le cadre du développement de nouveaux systèmes informatiques, le DPD travaille étroitement avec la DGA CIS (département informatique) pour améliorer et rendre compte de la participation du DPD aux stades précoces de la planification d'un nouvel outil informatique. Le but est de faciliter l'identification des risques d'atteinte à la vie privée et l'introduction de technologies améliorant le respect de la vie privée pour atténuer ces risques. La nécessité de telles technologies ou leur caractère adéquat sont identifiés par le biais de l'utilisation d'un modèle d'évaluation de l'impact sur la vie privée (PIA) qui permet au gestionnaire de projet et au DPD de se faire une idée des données à caractère personnel concernées et des principaux risques que présente le traitement.

En outre, le DPD siège au comité RH/informatique, qui est le comité chargé de planifier, d'approuver et de gérer tous les systèmes et applications informatiques pour les ressources humaines et l'administration du SGC»

#### AEAPP:

«- Réunion deux fois par mois avec le responsable du traitement (à savoir le directeur exécutif);

- Réunions mensuelles avec les cadres intermédiaires de l'unité de soutien aux entreprises (à savoir le chef d'unité, le chef d'équipe informatique et le chef d'équipe passation de marchés);

- Réunion mensuelle avec les cadres intermédiaires de l'équipe des RH (à savoir leur chef d'équipe);

- Participation aux demandes de plans de développement;

- Adoption/révision de procédures opérationnelles standard (comme la politique et la procédure) qui inclut un contrôle juridique du DPD;

- Mise en place de coordonnateurs de la protection des données au sein de chaque équipe de l'AEAPP et réunions régulières avec ces derniers;

- Organisation régulière de formations générales sur la protection des données ouvertes à tous les agents, qui sont toujours un excellent lieu d'échange pour partager des informations.

Le fait que le DPD ne soit pas un DPD à temps complet et qu'il soit membre de l'équipe juridique est considéré comme un avantage étant donné qu'il sera tenu informé des nouveaux traitements qui doivent être lancés.»

PE: «... Par sa nature et son organisation, le DPD participe régulièrement à l'élaboration et à la vérification de toutes les nouvelles décisions internes impliquant des données à caractère personnel...Le DPD participe aussi régulièrement à de nouveaux projets informatiques... En outre, des réunions régulières avec la hiérarchie et les CPD permettent au DPD d'être informé des nouveaux traitements. Enfin, des sessions de formation et d'information sont organisées deux ou trois fois par an avec les agents les plus concernés par les questions de protection des données dans les différentes DG».

Pour obtenir **un autre point de vue de parties prenantes** sur la question, le **CEPD a consulté les DPD de manière anonyme**, parmi lesquels (taux de participation d'environ 50 %) un peu plus de la moitié seulement ont indiqué qu'ils considéraient avoir été suffisamment consultés (17 «oui» contre 15 «non»). Dans l'ensemble, ils ont évalué leur satisfaction à 6,4 (sur une échelle allant de 0 -pratiquement jamais consulté- à 10 -toujours consulté-). Il y avait des commentaires encourageants («régulièrement associé aux décisions de toutes sortes»; «Bonne coopération entre le DPD et les domaines d'activité, bonne connaissance de la protection des données»; «Amélioration significative au cours des 18 derniers mois») et d'autres moins positifs («La consultation est cohérente et régulière, mais intervient trop tard dans le processus, il s'agit davantage de parer au plus pressé que de respecter la vie privée dès la conception») et des suggestions selon lesquelles, parfois, le DPD a été intentionnellement exclu ou du moins n'a pas été informé jusqu'à ce que certaines décisions soient devenues irréversibles, excluant de ce fait une véritable approche de respect de la vie privée dès la conception. La majorité des commentaires concernaient le fait d'être consulté sur les traitements (ou de les *découvrir*) trop tard dans le processus.



Lorsque le **type de participation** du DPD était précisé par les institutions, trois caractéristiques principales se distinguent: la participation au moyen d'une procédure définie et structurée (six institutions), la participation du DPD à des groupes de travail, des comités directeurs ou des réunions de la direction (13 cas, en particulier des comités directeurs informatiques = cinq) et en incluant la consultation du DPD comme une étape obligatoire dans les modèles de gestion de projets ou des cases à cocher sur la protection des données (quatre institutions).

Cela confirme les conclusions précédentes de l'enquête de 2013, dans laquelle le CEPD avait jugé que des réunions régulières avec les départements concernés (RH, informatique...) et l'inclusion d'une «case à cocher sur la protection des données» dans les modèles de gestion de projets étaient des façons particulièrement utiles de garantir l'implication adéquate du DPD. Les réponses ont également confirmé que plus l'institution est importante, plus les procédures sont susceptibles d'être formalisées. Là encore, plusieurs institutions ont mentionné d'autres tâches des DPD à temps partiel garantissant qu'elles soient tenues au courant de ce qui se passe (par exemple, rôles dans le service informatique ou conseiller juridique du directeur). Cela était notamment le cas dans les petites agences.

Le CEPD tient à rappeler que si cela peut fonctionner pour de plus petites agences ou des agences qui viennent d'être établies, **un processus de consultation plus formalisé semble être nécessaire pour les plus grandes organisations.**

EMA: «...une étape procédurale formelle est prévue qui vise à informer le délégué à la protection des données lorsqu'une nouvelle politique est proposée par les services compétents...En outre, des réunions bilatérales trimestrielles sont prévues entre le DPD et le Directeur exécutif pour examiner les questions relatives à l'application actuelle des politiques et à la conception de futures politiques/activités».

ERCEA: «Le DPD de l'ERCEA est membre du comité directeur informatique. Les instructions de l'ERCEA concernant l'élaboration et la validation de procédures internes (ICS8) prévoient explicitement la consultation à un stade précoce du DPD par les responsables des processus opérationnels avant de lancer la validation d'une procédure interne. En outre, le DPD doit être consulté sur tous les projets de procédures ou de modifications de ces procédures qui impliquent le traitement de données à caractère personnel (VISA requis dans la fiche de circulation ARES)...»

OHMI: «...l'étroite relation découle de notre règlement intérieur, mettant en œuvre le règlement (CE) n° 45/2001, qui constitue pour les responsables du traitement des données l'obligation de notifier au préalable le DPD de tout traitement de données à caractère personnel et de toute modification substantielle affectant toute donnée qui existe déjà. En particulier, dans chaque note interne envoyée au Président de l'Office, le département concerné doit compléter un champ, indiquant la «consultation du DPD». Cela favorise la consultation du DPD pour tous les projets et activités de l'Office, mais permet aussi aux responsables de l'Office d'avoir la garantie que les questions de protection des données ont été dûment couvertes lors de la présentation de la proposition à la présidence. En outre, le DPD est membre du Forum sur la sécurité de l'information. Le Forum est chargé de garantir la sécurité du traitement des données, à caractère personnel ou non, au sein de l'OHMI, conformément à la norme ISO 27001. ...».

Conseil: «La nécessité de telles technologies, ou leur caractère adéquat, sont identifiés par l'utilisation d'un modèle d'évaluation de l'impact sur la vie privée (PIA) qui permet au gestionnaire de projet et au DPD de se faire une idée des données à caractère personnel impliquées et des principaux risques que présente le traitement.»

«La protection des données dès la conception» est une bonne pratique. Elle permet de détecter les problèmes dès le processus de conception – évitant ainsi, par exemple, des

remaniements onéreux des logiciels à un stade ultérieur<sup>36</sup> – et d'intégrer une culture de protection des données dans le cycle de développement. **Le fait d'associer les DPD à un stade précoce de la conception de nouveaux traitements est une bonne façon de garantir le respect de la vie privée dès la conception.**

\*\*\*

Pour la majorité des DPD, leurs tâches font partie de leur **description de poste**. Ce n'est pas le cas pour six institutions seulement (AED, AESM, ERCEA, Eurofound, INEA, OSHA). Deux institutions (ERCEA, INEA) ont indiqué que le système existant de *description de postes* est trop générique pour tenir compte des spécificités du DPD, mais que ces spécificités (y compris le fait d'occuper le poste de DPD à temps partiel) ont été prises en considération dans le cadre des *objectifs* du DPD.

La grande majorité des institutions confirment que l'exécution des tâches du DPD fait partie de son **évaluation des performances**; ce n'est pas le cas pour quatre institutions seulement (CJUE, AED, AESM, Médiateur). Une institution fait part de ses préoccupations quant à l'indépendance du DPD si ses performances devaient être évaluées. Dans ce contexte, le CEPD a précisé dans le **document de référence sur le rôle joué par les DPD**<sup>37</sup> que si le DPD ne peut recevoir d'instructions, cela n'exclut pas une évaluation de ses performances. Cependant, en raison de l'indépendance du DPD, «...le **DPD ne devrait rendre des comptes qu'à l'autorité qui l'a désigné, et non à un supérieur direct**»<sup>38</sup>.

Les **Normes professionnelles des délégués à la protection des données**<sup>39</sup> publiées en 2010 par le Réseau des délégués à la protection des données des institutions et organes de l'UE donnent des orientations supplémentaires sur la question, en particulier pour les **DPD à temps partiel**:

- Page 6, le document explique: «Un DPD qui rend compte à un supérieur direct dans la hiérarchie (directeur ou chef d'unité) et qui est évalué par ce dernier peut ressentir une pression à coopérer et à bien s'entendre avec la direction et d'autres collègues, étant donné qu'une exécution dynamique des tâches de DPD peut avoir des répercussions négatives sur la carrière. Si le DPD veut s'acquitter correctement de ses tâches, il doit souvent se montrer ferme et insistant, également avec les responsables du traitement haut placés dans l'organisation, ce qui peut l'amener à être perçu, au mieux, comme un bureaucrate ou, au pire, comme un 'fauteur de troubles' déplaisant. En conséquence, le DPD doit être en mesure de résister à la pression et de faire face aux difficultés qui vont de pair avec cette fonction importante. Pour réduire cette pression, le DPD doit rendre compte au chef d'administration de l'institution ou de l'organe et être évalué par ce dernier. Cet aspect revêt une importance particulière pour le DPD à temps partiel qui doit directement rendre compte à l'autorité qui l'a désigné en ce qui

---

<sup>36</sup> Une institution a explicitement mentionné ce problème, indiquant que c'était moins le cas pour les systèmes associés aux RH maintenant que le DPD participe régulièrement au comité directeur des RH/informatique.

<sup>37</sup> Document de référence sur le rôle joué par les délégués à la protection des données pour garantir le respect effectif du règlement (CE) n° 45/2001, voir [https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Papers/PositionP/05-11-28\\_DPO\\_paper\\_FR.pdf](https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Papers/PositionP/05-11-28_DPO_paper_FR.pdf).

<sup>38</sup> Document de référence sur le rôle joué par les délégués à la protection des données pour garantir le respect effectif du règlement (CE) n° 45/2001, p. 8.

<sup>39</sup> Normes professionnelles des délégués à la protection des données des institutions et organes de l'UE qui travaillent en application du règlement (CE) n° 45/2001, publiées par le Réseau des délégués à la protection des données des institutions et organes de l'UE, voir [http://ec.europa.eu/dataprotectionofficer/docs/dpo\\_standards\\_en.pdf](http://ec.europa.eu/dataprotectionofficer/docs/dpo_standards_en.pdf).

concerne ses fonctions de DPD, et à son supérieur hiérarchique pour ce qui est des autres fonctions, et être évalué par ces derniers».

- Page 7, le document précise notamment que «... Lorsqu'il évalue les performances du DPD, l'évaluateur doit veiller à ne pas réprimander le DPD si celui-ci a pris des positions impopulaires ni à considérer les obligations en matière de protection des données comme une charge administrative. Pour un DPD à temps partiel, la même importance doit être accordée à l'exécution de ses tâches de DPD et à l'exécution de ses autres tâches. Si les dispositions d'application de l'institution/organe le prévoient, le CEPD doit avoir la possibilité de donner son avis sur les performances du DPD».

Les exemples cités par les institutions dans leurs réponses à l'enquête de 2015 illustrent le fait que ces recommandations ont été bien intégrées dans le processus d'évaluation de nombreux DPD:

CdT: «L'évaluation des performances du DPD fait l'objet de deux processus d'évaluation, le premier mené par le Directeur (concernant uniquement les tâches du DPD) et le deuxième par le supérieur hiérarchique.»

Cedefop (DPD à temps partiel): «...deux évaluations des performances séparées et distinctes réalisées par différents évaluateurs, l'une pour la fonction de DPD et la deuxième pour l'autre fonction du poste.»

ABE: «L'évaluation est réalisée par le cadre moyen du DPD, avec la contribution du Directeur exécutif en ce qui concerne les fonctions de la personne en tant que DPD.»

ECDC: «Les performances concernant les tâches du DPD comptent autant que les performances concernant les tâches qui n'incombent pas au DPD. Étant donné que le DPD rend compte directement au Directeur, l'évaluation des performances concernant les tâches du DPD est réalisée par le Directeur. Ces règles ont été formalisées en interne.»

EMA: «...le supérieur hiérarchique...consulte le Directeur exécutif concernant l'évaluation des performances du DPD et reçoit sa contribution/ses commentaires avant de finaliser le rapport.»

Dès lors que toutes les institutions indiquent que leur DPD est associé à la conception de nouveaux traitements, le **CEPD invite toutes les institutions à s'assurer que les activités du DPD sont évaluées dans le cadre de l'évaluation des performances du DPD.**

À son tour, le CEPD encourage les DPD à élaborer leurs propres principes communs de bonne supervision (exigences, programme de travail annuel, rapport annuel...) qui peuvent servir à mesurer les résultats de leurs travaux<sup>40</sup>.

## 2.6. Organes qui n'ont pas répondu à l'enquête

Au moment de l'adoption du présent texte, seul un organe, l'EC SESAR, n'avait pas répondu à l'enquête sur le fond.

L'EC SESAR a relevé un «manque de moyens» en raison de l'obligation de désigner un DPD faisant fonction.

Il n'en demeure pas moins que le règlement doit être respecté. Comme mentionné dans l'introduction, les résultats de la présente enquête alimenteront la planification des mesures

<sup>40</sup> Voir aussi Document de référence sur le rôle joué par les délégués à la protection des données pour garantir le respect effectif du règlement (CE) n° 45/2001, p. 8.

d'application pour 2016. Lorsque des institutions de l'UE ne répondent pas dans les délais impartis, il y a lieu de s'inquiéter.

### 3. Suivi de l'enquête précédente: visites de contrôle

#### 3.1. Remarques générales

À la suite de l'enquête précédente – hormis le suivi général et certains cas spécifiques – le CEPD a rendu visite à cinq institutions épinglées lors de l'exercice de 2013.

À l'époque, une visite d'inspection en tant que telle n'était pas envisagée pour ces institutions parce que le niveau de respect du règlement (CE) n° 45/2001 était généralement faible. Il était impossible de «contrôler la réalité» de traitements qui n'avaient pas encore été notifiés ou d'outils de contrôle du respect de la réglementation (inventaire, registre) qui n'existaient pas, en raison de l'absence d'attentes à contrôler.

Ces visites de contrôle servent à veiller au respect du règlement par les cadres supérieurs et intermédiaires. Cette approche «descendante» vise à garantir l'adhésion des cadres. L'expérience a démontré qu'une protection des données efficace n'était pas seulement une question de ressources, mais aussi de volonté de l'organisation. Autrement dit, ces visites sont des «visites courtoises, mais pas des visites de courtoisie». L'instrument qui constitue ces visites de contrôle a depuis été codifié à l'article 36 du règlement intérieur du CEPD<sup>41</sup>.

**Visites de contrôle:** Une visite est un outil de contrôle, dont le but est d'obtenir l'engagement des instances dirigeantes d'une institution ou d'une agence à respecter le règlement. La décision d'organiser une visite est généralement prise en cas de non-respect des règles relatives à la protection des données, de communication insuffisante ou simplement pour sensibiliser l'institution concernée au respect de la réglementation. Elle est fondée sur les informations que nous avons rassemblées lors d'un exercice de contrôle de la conformité, dans une enquête générale par exemple. La visite comprend une visite sur place effectuée par le CEPD ou le Contrôleur adjoint; elle est suivie d'une correspondance concernant une feuille de route spécifique convenue entre nous et l'organe visité.

Pour améliorer le respect de la réglementation, le CEPD a profité de ces visites pour établir des feuilles de route précises en accord avec la hiérarchie de l'institution concernée. Ces feuilles de route comprennent des objectifs et des délais spécifiques: établissement d'un inventaire, progrès à accomplir quant au niveau de notifications au titre des articles 25 et 27, notification de procédures ciblées pour lesquelles le CEPD a publié des lignes directrices<sup>42</sup>, et autres questions propres à l'institution visitée (pérenniser la fonction de DPD, former le personnel à la protection des données, etc.).

Comme lors du précédent exercice, une comparaison des taux de notification entre l'enquête de 2013 et les résultats actuels a été effectuée en vue d'évaluer les effets de ces visites.

Nom	Résultats de l'enquête de 2015		Résultats de l'enquête de 2013		Variation des taux	
	Article 25	Article 27	Article 25	Article 27	Article 25	Article 27
EIGE	50%	86%	63%	86%	-13	+/- 0

<sup>41</sup> [http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32013D0504\(03\)&from=FR](http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32013D0504(03)&from=FR).

<sup>42</sup> <https://secure.edps.europa.eu/EDPSWEB/edps/site/mySite/Guidelines>.

<b>FEI</b>	34%	47%	<b>Non comparable</b>		-	-
<b>GSA (GNSS)</b>	52%	54%	<b>Non comparable</b>			
<b>CSUE</b>	52%	100%	<b>Pas de réponse</b>			
<b>IESUE</b>	25%	17%	<b>0%</b>	<b>0%</b>	<b>+25</b>	<b>+17</b>

**Graphique 4: Évolution des taux de notification pour les agences visitées**

Le tableau ci-dessus montre les pourcentages pour les notifications au titre des articles 25 et 27 tant en 2013 qu'en 2015, pour chacune des institutions visitées, ainsi que les variations au niveau de ces points de pourcentage. Il confirme que les visites ont un effet clairement positif sur le respect de la réglementation. Les sections ci-après fournissent des informations complémentaires sur chacune des visites et des améliorations constatées par la suite.

### **3.2. EIGE**

L'Institut européen pour l'égalité entre les hommes et les femmes (EIGE), basé à Vilnius, a officiellement commencé ses activités durant l'été 2010. La réponse de l'EIGE à l'enquête de 2011 était parvenue trop tard et, début 2013, il n'avait toujours pas notifié de traitements pouvant être soumis au contrôle préalable. C'est pour cette raison que le contrôleur adjoint lui a rendu visite en mai 2013. Lors de la visite qui a duré une demi-journée, le contrôleur adjoint a rencontré la direction, le personnel chargé des traitements, ainsi que le DPD et le DPD adjoint. À la suite de cette visite, l'EIGE et le CEPD ont convenu d'une feuille de route en vue d'une mise en conformité. Pour une agence de son âge, l'EIGE a enregistré de bons résultats dans l'enquête de 2013 et a également fait le point sur les autres éléments de la feuille de route. Cependant, les taux de notification au titre de l'article 25 ont baissé depuis l'enquête de 2013, ce qui indique que l'effort initialement fourni n'a peut-être pas été maintenu.

### **3.3. FEI**

Le Fonds européen d'investissement (FEI) est un partenariat public-privé avec la BEI, la Commission européenne et plusieurs institutions financières comme des actionnaires basés au Luxembourg. Son activité principale est le financement à risque des PME. La décision de visiter le FEI reposait sur un réexamen des rôles correspondants concernant le traitement de données entre le FEI et la BEI, qui n'étaient pas suffisamment clairs, et l'identification consécutive de faibles taux de notification dans l'enquête de 2013 pour les traitements du FEI qu'il gère lui-même (indépendamment de la BEI). Au cours de la visite, nous avons identifié plusieurs domaines de non-conformité, par exemple, en ce qui concerne la clarté de l'inventaire et l'absence de notifications au titre des articles 25 et 27 du règlement. Le FEI s'est engagé à prendre des mesures pour parvenir à la conformité dans le cadre d'une feuille de route convenue d'un commun accord. Entre-temps, il a complété l'inventaire, mis à jour le registre de l'article 25 et déposé une série de notifications au titre de l'article 27 auprès du CEPD. Les chiffres dans la section 2.1 reflètent la situation à la date où le FEI a soumis sa réponse à l'enquête - depuis, le FEI a rattrapé son retard et est en bonne voie de finaliser la feuille de route.

### **3.4. CSUE (Centre satellitaire de l'UE) et GSA (Agence du GNSS européen)**

Le Centre satellitaire de l'UE et l'Agence du GNSS européen (GSA) ont également été sélectionnés pour une visite, sur la base de notre enquête 2013, où nous avons constaté que la communication posait problème. Étant donné qu'aucune des deux agences n'a fourni

suffisamment de preuves pour démontrer qu'elle respectait pleinement la réglementation d'ici le délai fixé, nous avons décidé d'effectuer ces visites au niveau opérationnel sur des questions allant de la gestion des ressources humaines à la sécurité informatique en passant par les tâches des différents acteurs au sein de l'organisation en ce qui concerne la protection des données. Cela s'est traduit par des formations et des sessions de Q&R organisées par les agents du CEPD chargés des dossiers, dans le but d'aider l'agence sur des aspects pratiques et d'éduquer le personnel et la direction sur la manière d'intégrer au mieux les principes de protection des données dans leur environnement de travail. Les deux agences ont établis de solides contacts avec nous et nous ont fait part de leur engagement à améliorer le respect des principes de protection des données - toutes deux en vue de devenir pleinement conformes pour la présente enquête 2015. Alors que la coopération avec la GSA s'est améliorée, les niveaux de notification sont restés en-deçà de la moyenne pour une agence de son âge à la date limite fixée pour répondre à la présente enquête. Cependant, plusieurs nouvelles notifications au titre de l'article 27 ont été soumises avant la date de publication du présent rapport. En ce qui concerne le Centre satellitaire de l'UE, un membre du personnel du CEPD a été détaché en novembre 2014, et une réunion au niveau de la direction s'est tenue en décembre 2014. Depuis lors, toutes les notifications au titre de l'article 27 ont été soumises et presque tous les dossiers sont clos. En ce qui concerne les notifications spécifiques à l'informatique, une étroite coopération avec le CEPD sera assurée en tant que de besoin.

### **3.5. IESUE**

L'Institut d'études de sécurité de l'Union européenne (IESUE) a été épinglé pour une visite en raison de ses résultats dans l'enquête de 2013. Ancienne agence de second pilier, l'IESUE a mis à jour sa base juridique début 2014. Pour des raisons pratiques, la visite a été organisée en deux temps: une réunion entre le directeur de l'IESUE et le contrôleur adjoint en juin 2014, et une visite à l'IESUE à Paris au niveau du personnel en octobre 2014. Lors de la réunion entre le directeur et le contrôleur adjoint, l'IESUE s'est engagé à améliorer la conformité. Pendant la visite à Paris, le personnel du CEPD a rencontré le nouveau chef de l'administration de l'IESUE, le DPD et le personnel concerné pour discuter et organiser une session de formation sur les principes de protection des données. La présente enquête 2015 sera utilisée pour mesurer l'amélioration de la conformité de l'IESUE. Alors que l'IESUE a commencé à travailler sur sa conformité, les niveaux de notification restent faibles, même pour une agence dont la fonction de protection des données est récente (le premier DPD de l'IESUE a été désigné à la suite de l'enquête de 2013). Des efforts supplémentaires doivent être consentis, notamment par les unités opérationnelles, pour respecter leur obligation de notification au DPD.

### **3.6. Évaluation du programme des visites**

Comme c'était le cas pour la précédente enquête, les résultats montrent que les visites ont été un instrument utile pour améliorer le respect de la réglementation en fournissant des informations, en sensibilisant les cadres supérieurs et en convenant de délais et objectifs concrets pour la plupart des organes visités. Le programme se poursuivra donc dans les années à venir. Les résultats de la présente enquête constitueront également un facteur important pour déterminer les institutions de l'UE à visiter à l'avenir.

La plupart des visites ont conduit à une amélioration du respect de la réglementation; toutefois, si une visite ne débouche pas sur des changements positifs, d'autres actions de suivi doivent être envisagées. Dans ces cas, le CEPD peut décider de réaliser une inspection ou de

faire usage des compétences d'application que lui confère l'article 47, paragraphe 1, du règlement<sup>43</sup>.

---

<sup>43</sup> Voir le document stratégique du CEPD sur «Les inspections menées par le CEPD» ([https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Inquiries/2013/13-11-04\\_EDPS\\_Inspection\\_Policy\\_FR.pdf](https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Inquiries/2013/13-11-04_EDPS_Inspection_Policy_FR.pdf)), p. 5.

#### 4. Conclusions et suivi prévu

Dans l'ensemble, les résultats de l'enquête de cette année attestent une fois de plus de progrès constants consentis en vue de la mise en œuvre intégrale du règlement par les institutions de l'UE.

En ce qui concerne les institutions bien établies et matures, peu de choses ont changé en termes de réponses - les taux de notification sont élevés et la fonction du DPD est consolidée. Le défi à relever par ces institutions de l'UE reste la bonne tenue de l'inventaire et du registre. Dans certains cas, les taux de notification ont légèrement baissé en raison de l'établissement de nouveaux traitements. Rien d'alarmant en soi, mais cela démontre que le maintien des inventaires et des registres exige une attention constante et n'est pas un exercice ponctuel. Ces institutions de l'UE doivent désormais s'assurer de généraliser la protection des données, afin qu'elle devienne un réflexe.

Les résultats du groupe B sont similaires. En ce qui concerne les notifications au titre de l'article 27, l'écart a été comblé par rapport au groupe A; pour ce qui est de l'article 25, un faible écart subsiste. Les agences qui étaient à la traîne ont également rattrapé leur retard, comme l'AESA. Plusieurs agences ont fait un sans faute et plusieurs autres agences ont raté leur objectif à quelques notifications près.

Le groupe C affiche désormais des taux de notification moyens meilleurs que ceux du groupe B lors de l'enquête de 2013 et a presque rattrapé ce groupe dans le cadre de la présente enquête. L'INEA est un exemple de réussite, ainsi que Frontex, qui affiche aujourd'hui de solides résultats compris dans la moyenne alors qu'il était autrefois source de préoccupations.

Il est compréhensible que le groupe D enregistre des taux plus faibles. Cependant, après les améliorations spectaculaires constatées entre l'enquête de 2011 et celle de 2013, les progrès semblent avoir ralenti, notamment en ce qui concerne les notifications au titre de l'article 27. Le CEPD fournira si nécessaire une aide et un tutorat afin de garantir le respect adéquat du règlement.

La présente enquête n'a pas uniquement pour but de présenter un état de la situation sur la mise en œuvre du règlement. Elle alimente aussi les choix du CEPD en ce qui concerne les activités de supervision et d'application des règles.

Il ressort des résultats de l'enquête que plusieurs organes rencontrent encore des problèmes pour appliquer le règlement.

Outre les visites, le CEPD pourrait envisager l'adoption d'autres mesures d'application inspirées par les compétences conférées par le règlement.



## IV. Annexe 1) Méthodologie

Comme lors des précédents exercices, l'enquête a pris la forme d'un exercice analytique, invitant les institutions de l'UE à fournir des informations par écrit. La liste des questions a été envoyée aux institutions de l'UE en avril 2015; des rappels ont été envoyés en juin 2015 au niveau opérationnel. Les réponses sont parvenues tout au long des mois de juin et juillet 2015. En décembre 2015, le projet de rapport a été soumis pour consultation aux institutions de l'UE.

Les institutions de l'UE ont été invitées à fournir des informations sur les aspects suivants:

1. **Inventaire et registre**<sup>44</sup>: le nombre de traitements 1) identifiés dans l'inventaire, 2) ceux notifiés au DPD et inclus dans le registre, 3) ceux identifiés comme relevant de l'article 27 et 4) ceux qui ont déjà été notifiés au CEPD au titre de l'article 27<sup>45</sup>;
2. **Transferts de données à caractère personnel relevant de l'article 9** au cours des années 2013 et/ou 2014:
  - transferts relevant de l'article 9, paragraphes 2, 6 ou 7 et transferts relevant de l'article 9 à des destinataires qui sont établis dans des pays de l'EEE, mais qui réalisent des types d'activités qui sont exclus de l'application de la directive 95/46/CE;
  - précisions sur le traitement (tel que mentionné dans la notification au titre de l'article 25), le destinataire, la base, le domaine (par exemple, application de la loi), le «comment» du transfert, les catégories de données à caractère personnel ainsi que la fréquence de ces transferts;
  - toute difficulté particulière rencontrée dans les activités ci-dessus;
  - existence d'un système interne de contrôle et d'enregistrement des transferts relevant de l'article 9;
3. **Sécurité de l'information**: 1) existence d'un processus spécialement dédié à la sécurité de l'information, 2) réalisation d'évaluations des risques, 3) existence d'une politique de sécurité générale<sup>46</sup>, 4) existence d'un processus formel pour faire face aux incidents de sécurité et 5) notification ou non du DPD lorsque l'incident de sécurité de l'information implique des données à caractère personnel.
4. **Garantir l'effacement effectif des données à caractère personnel**: 1) existence d'une politique écrite et d'une procédure standard régissant l'effacement effectif des données à caractère personnel à la fin du délai de conservation, 2) existence de processus automatisés soutenant la procédure d'effacement dans tous les systèmes, 3) mesures destinées à garantir l'effacement des informations dans les copies de sauvegarde, le cas échéant.
5. **Votre délégué à la protection des données et vous**: dans une section séparée, pour laquelle le CEPD a explicitement demandé que ce ne soit *pas* le DPD qui fournisse les réponses, le CEPD a demandé des informations pour savoir si les tâches du DPD font partie de la description de son poste, si l'exécution des tâches du DPD fait partie de

<sup>44</sup> Contrairement aux exercices précédents, le CEPD n'a pas demandé à recevoir les copies de l'actuel inventaire ou registre.

<sup>45</sup> Lorsque ces informations sont également disponibles de manière plus détaillée, par exemple, par direction générale de l'institution ou de l'organe, les institutions de l'UE ont été invitées à fournir ces informations également.

<sup>46</sup> Cette question ne concernait pas des politiques de sécurité spécifiques à l'application.

l'évaluation de ses performances et comment le DPD participe à la conception de nouveaux traitements.

Un aperçu des réponses apportées à la question 1 est fourni dans un tableau comparatif (voir section **Error! Reference source not found.** ci-dessus). Les questions 2 à 5, qui ne se prêtent pas facilement à une analyse quantitative, sont analysées qualitativement dans le corps du présent rapport.

## V. Annexe 2) Limites de la méthodologie

- I. Une institution qui n'identifie pas correctement toutes les procédures impliquant des traitements peut avoir un taux faussement élevé de respect de la réglementation.
- II. Il est possible que les inventaires contiennent déjà des procédures impliquant des traitements identifiés par l'institution mais pas encore totalement développées. À l'évidence, la procédure ne peut être notifiée avant d'avoir été suffisamment développée. Le calcul la fait toutefois apparaître comme un traitement non notifié et met donc en évidence un niveau plus faible de notification.
- III. Une institution peut identifier dans son inventaire un futur traitement à risque, mais comme la procédure liée à ce traitement n'est pas encore suffisamment développée, il ne peut être notifié conformément à l'article 27. Le calcul la fait apparaître comme un traitement non notifié et met donc en évidence un niveau plus faible de notification.
- IV. À l'inverse, les institutions qui identifient de nombreux traitements supplémentaires peuvent voir leur taux de notification baisser, malgré les efforts considérables déployés pour effectuer les notifications. Cet effet de «course en avant» est mentionné lorsqu'il a pu être observé.
- V. De même, le fait de mettre à jour les notifications peut se traduire par une baisse temporaire des taux de notification. Pour les notifications au titre de l'article 25, lorsque de telles baisses ont pu être observées, le CEPD a demandé des éclaircissements; il s'agit souvent de modifications mineures (par exemple, un nouveau chef d'unité comme point de contact), elles ont donc été comptabilisées comme étant effectuées, pour éviter de pénaliser les institutions qui ont fait un effort pour maintenir leur registre à jour. Pour les notifications au titre de l'article 27, lorsque les mises à jour nécessitent des notifications actualisées ou de nouvelles notifications à envoyer au CEPD, ces dernières ont été comptabilisées comme non effectuées. Le cas échéant, cela est mentionné dans le rapport.
- VI. Le CEPD peut suspendre l'analyse d'une notification si des lignes directrices sont en cours d'élaboration sur la même procédure. Le calcul peut toutefois la faire apparaître comme traitement non notifié et donc mettre en évidence un niveau plus faible de respect de la réglementation. Si le CEPD reçoit des notifications sur ces traitements avant la publication des lignes directrices, ils seront considérés comme ayant été notifiés. Seule leur analyse sera suspendue.

## VI. Annexe 3) Groupes d'institutions de l'UE

**Groupe A (12):** institutions fondées avant 2004 et ayant désigné un DPD avant l'établissement du CEPD:

Commission européenne, Comité des régions, Conseil, Cour des comptes européenne, Banque centrale européenne, Cour de justice de l'Union européenne, Comité économique et social européen, Banque européenne d'investissement, Parlement européen, OLAF, Médiateur européen et Centre de traduction des organes de l'Union européenne.

**Groupe B (17):** organes établis (ou ayant commencé leurs activités) en 2004 ou antérieurement, mais ayant désigné un DPD ultérieurement:

Cedefop, OCVV, EASME, AESA, CEPD, AEE, EFSA, FEI, OEDT, EMA, EMSA, ENISA, ETF, Eurofound, FRA, OHMI et EU-OSHA.

**Groupe C (18):** organes établis (ou ayant commencé leurs activités) après 2004 mais avant 2011:

AECP, EACEA, Chafea, ECDC, ECSEL (successeur d'ARTEMIS et de l'ENIAC), AFE, FRONTEX, GSA, INEA, EC Clean Sky, ECHA, ERCEA, F4E, EC PCH, EC IMI, REA, SESAR.

**Groupe D (15):** organes établis (ou ayant commencé leurs activités) en 2011 ou ultérieurement, ainsi que les anciens organes des deuxième et troisième piliers:

ACER, ORECE, EASO, ABE, AEAPP, EIGE, EIT, AEMF, CERS, SEAE, eu-LISA, CEPOL, AED, IESUE, CSUE.

## VII. Annexe 4) Liste des acronymes des institutions

ACER	Agence de coopération des régulateurs d'énergie
ORECE	Organe des régulateurs européens des communications électroniques
CdT	Centre de Traduction des organes de l'Union européenne
Cedefop	Centre européen pour le développement de la formation professionnelle
CEPOL	Collège européen de police
CHAFEA	Agence exécutive pour les consommateurs, la santé et l'alimentation
CJUE	Cour de justice de l'Union européenne
EC Clean Sky	Entreprise commune Clean Sky
CdR	Comité des régions
Conseil	Conseil de l'Union européenne
CE	Commission européenne
OCVV	Office communautaire des variétés végétales
EACEA	Agence exécutive «Éducation, audiovisuel et culture»
AESA	Agence européenne de la sécurité aérienne
EASME	Agence exécutive pour les petites et moyennes entreprises
EASO	Bureau européen d'asile en matière d'appui
ABE	Autorité bancaire européenne
CC	Cour des comptes européenne
BCE	Banque centrale européenne
ECDC	Centre européen de prévention et de contrôle des maladies
ECHA	Agence européenne des produits chimiques
EC ECSEL	Entreprise commune «Composants et systèmes électroniques pour un leadership européen»
AED	Agence européenne de défense
CEPD	Contrôleur européen de la protection des données
AEE	Agence européenne pour l'environnement
SEAE	Service européen pour l'action extérieure
CESE	Comité économique et social européen
AECP	Agence européenne de contrôle des pêches
EFSA	Autorité européenne de sécurité des aliments
BEI	Banque européenne d'investissement
FEI	Fonds européen d'investissement
EIGE	Institut européen pour l'égalité entre les hommes et les femmes
AEAPP	Autorité européenne des assurances et des pensions professionnelles
EIT	Institut européen d'innovation et de technologie
EMA	Agence européenne des médicaments
OEDT	Observatoire européen des drogues et des toxicomanies
AESM	Agence européenne pour la sécurité maritime
ENISA	Agence de l'Union européenne chargée de la sécurité des réseaux et de l'information
PE	Parlement européen
AFE	Agence ferroviaire européenne
ERCEA	Agence exécutive du Conseil européen de la recherche
CERS	Comité européen du risque systémique
AEMF	Autorité européenne des marchés financiers
ETF	Fondation européenne pour la formation
IESUE	Institut d'études de sécurité de l'Union européenne
eu-LISA	Agence européenne pour la gestion opérationnelle des systèmes d'information à grande échelle au sein de l'espace de liberté, de sécurité et de justice
EUROFOUND	Fondation européenne pour l'amélioration des conditions de vie et de travail
CSUE	Centre satellitaire de l'Union européenne
F4E	Fusion for Energy
FRA	Agence des droits fondamentaux de l'Union européenne
Frontex	Agence européenne pour la gestion de la coopération opérationnelle aux frontières extérieures des États membres de l'Union européenne
EC PCH	Entreprise commune Piles à combustible et Hydrogène
GSA (GNSS)	Autorité du GNSS européen
EC IMI	Entreprise commune Initiative en matière de médicaments innovants
INEA	Agence exécutive pour l'innovation et les réseaux
OHMI	Office de l'harmonisation dans le marché intérieur (marques, dessins et modèles)
OLAF	Office européen de lutte antifraude
Médiateur	Médiateur européen
EU-OSHA	Agence européenne pour la sécurité et la santé au travail
REA	Agence exécutive pour la recherche
EC SESAR	Entreprise commune Système européen de nouvelle génération pour la gestion du trafic aérien