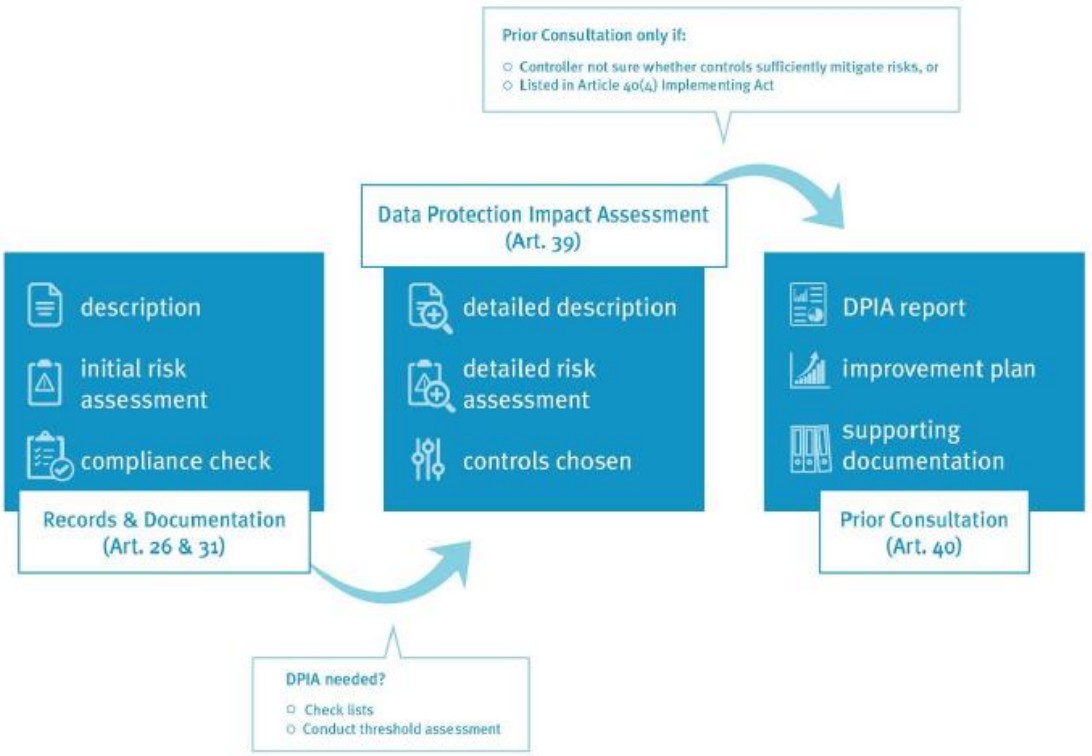
LE CONTRÔLEUR EUROPÉEN DE LA PROTECTION DES DONNÉES (CEPD)

Responsabilisation sur le terrain: lignes directrices relatives à la documentation des opérations de traitement pour les institutions, organes et agences de l'UE

Résumé

v1.3 Juillet 2019



Prior Consultation only if:	Consultation préalable uniquement si:
Controller not sure whether controls sufficiently mitigate risks, or Listed in Article 40 (4) Implementing Act	Le responsable du traitement n'est pas certain que les mesures de maîtrise des risques atténuent suffisamment ceux-ci, ou Répertoriés dans un acte d'exécution au titre de l'article 40, paragraphe 4
Data Protection Impact Assessment (Art. 39)	Analyse d'impact relative à la protection des données (article 39)
description	dans l'affirmative, description
initial risk assessment	Évaluation des risques initiale
compliance check	Contrôle de conformité
Records & Documentation (Art. 26 &31)	Registres et documentation (articles 26 et 31)
detailed description	Description détaillée
detailed risk assessment	Évaluation des risques détaillée
controls chosen	Mesures de maîtrise des risques choisies
DPIA report	Rapport d'AIPD
improvement plan	Plan d'amélioration
supporting documentation	Documents justificatifs
Prior Consultation (Art. 40)	Consultation préalable (article 40)
DPIA needed?	AIPD nécessaire?
Check lists	Listes de contrôle
Conduct threshold assessment	Réaliser une analyse de seuil

1 Responsabilisation sur le terrain

Lorsqu'ils traitent des informations relatives à des personnes («données à caractère personnel»), les institutions, organes et agences de l'UE (IUE) doivent se conformer à certaines règles afin de protéger la vie privée de celles et ceux dont ils sont amenés à traiter les données. Ce principe s'applique aux données de leur propre personnel, mais aussi à celles de bénéficiaires, de sous-traitants ou de toute autre personne. Le règlement (UE) 2018/1725[1] (ci-après le «règlement») fixe les règles applicables aux IUE.

En bref, ces règles vous disent ceci:

(1) vous devez avoir une bonne raison de traiter les données des personnes,
(2) vous devez les en informer,
(3) vous êtes responsable de *ce que* vous faites et *de la raison* pour laquelle vous le faites.

Les principaux acteurs, c'est vous, dans les IUE, vous qui êtes responsables du traitement des données à caractère personnel («responsables du traitement»). **Vous êtes comptable de ce que vous faites et des raisons pour lesquelles vous le faites de cette façon**. Cela suppose de se conformer à la réglementation en vigueur, mais aussi de pouvoir le **prouver**.

La meilleure façon de le faire consiste à suivre une **approche structurée pour concevoir et documenter les opérations de traitement**. Cela signifie également que vous devez y penser dès la conception de vos nouveaux processus («prise en compte du respect de la vie privée dès la conception»). La boîte à outils du Contrôleur européen de la protection des données (CEPD) *Responsabilisation sur le terrain: lignes directrices relatives à la documentation des opérations de traitement pour les institutions, organes et agences de l'UE* fournit des orientations dans ce sens. Celles-ci sont résumées dans la présente brochure. Ce processus de conception et de documentation des opérations de traitement n'est pas une fin en soi, mais un **moyen d'atteindre un objectif**: être transparent, conforme et responsable.

Le règlement s'appuie sur des règles antérieures adoptées en 2001 [règlement (CE) 45/2001[2] (ci-après l'«ancien règlement»)] et reflète le règlement général sur la protection des données (UE) 2016/679 (RGPD)[3], qui s'applique à la plupart[4] des organisations traitant des données à caractère personnel («responsables du traitement») dans les États membres – qu'il s'agisse d'administrations publiques, d'entreprises, d'associations caritatives ou d'autres organisations. Par rapport aux règles précédentes, **le nouveau règlement met davantage en adéquation vos obligations documentaires avec les risques posés par le traitement de données à caractère personnel**. Ainsi, les exigences documentaires concernant un abonnement au bulletin d'information de votre IUE seront moins strictes que celles applicables à un système de vidéosurveillance qui couvre un espace accessible au public. Ces règles tiennent en outre compte du statut de «droit fondamental» qu'a acquis la protection des données en vertu de l'article 8 de la charte des droits fondamentaux de l'UE.

Les IUE doivent montrer l'exemple en matière de droits fondamentaux, y compris dans le domaine de la protection des données. Le **CEPD, l'autorité de contrôle chargée de vérifier la manière dont les IUE traitent les données à caractère personnel, fournit des orientations détaillées sur de nombreux aspects du respect de ces règles.**

La présente boîte à outils traite de la situation spécifique des institutions européennes placées sous la supervision du CEPD, mais elle est conforme aux principes du RGPD et aux lignes directrices publiées

[1] JO L 295 du 21.11.2018, p. 39.
[2] JO L 8 du 12.1.2001, p. 1.
[3] JO L 119 du 4.5.2016, p. 1.
[4] Le traitement à des fins répressives par les autorités compétentes des États membres est quant à lui soumis à la mise en œuvre nationale de la directive 2016/680; JO L 119 du 4.5.2016, p. 89.

par le groupe de travail «article 29» (GT29) et le Comité européen de la protection des données[5]. Le cas échéant, nous la mettrons à jour afin qu'elle reste cohérente avec l'interprétation que fait le Comité européen de la protection des données du RGPD. Elle peut donc également être utile à des responsables du traitement, des délégués à la protection des données (DPD) et d'autres parties intéressées en dehors des IUE. Les règles applicables aux IUE étant équivalentes à celles du RGPD, elles doivent également être interprétées de la même manière. Raison pour laquelle nous nous référerons aussi occasionnellement au RGPD.

Si vous souhaitez en savoir plus, **parlez-en au DPD de votre IUE** et explorez la boîte à outils. Les références entre crochets dans la présente brochure vous indiqueront où trouver de plus amples informations dans la boîte à outils. Pour des conseils sur d'autres sujets, et par exemple sur le moment où informer les personnes que vous traitez leurs données et comment, ou sur les aspects relatifs à la protection des données de processus métier spécifiques (recrutement, évaluation du personnel, enquêtes administratives et procédures disciplinaires, etc.), veuillez consulter le site web du CEPD[6].

2 Public cible, domaine d'application et relation avec d'autres documents

La **présente boîte à outils s'adresse plus particulièrement aux responsables du traitement et au personnel compétent pour leur compte, aux DPD, aux coordinateurs de la protection des données** (CPD)[7] et à toute autre personne active dans la conception et la gestion d'activités de traitement de données à caractère personnel au sein des IUE. Dans les IUE, le responsable du traitement est, juridiquement parlant, «l'institution ou l'organe de l'Union ou la direction générale ou toute autre entité organisationnelle qui, seule ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données à caractère personnel»[8].

Aux fins de la présente boîte à outils, le terme «vous» désigne la «personne compétente pour le compte du responsable du traitement» ou le «responsable du traitement dans la pratique» (propriétaire de processus) d'une opération de traitement existante, ou le propriétaire du projet pour les activités en cours d'élaboration.

La présente boîte à outils fournit des orientations sur la manière de se conformer au règlement dans les domaines de la documentation en matière de protection des données et des analyses des risques à effectuer pour les opérations de traitement «à risque». Elle couvre les aspects suivants et fournit des modèles pour la plupart d'entre eux:

- comment documenter vos activités de traitement,
- quand réaliser une analyse d'impact relative à la protection des données (AIPD),
- comment réaliser des AIPD,
- quand envoyer une AIPD au CEPD pour consultation préalable,
- qui fait quoi dans les processus ci-dessus,
- les règles de transition depuis l'ancien règlement applicables aux institutions de l'UE en matière de protection des données.

[5] Par exemple, les lignes directrices concernant l'analyse d'impact relative à la protection des données (AIPD) et la manière de déterminer si le traitement est «susceptible d'engendrer un risque élevé» aux fins du règlement (UE) 2016/679, WP248, disponibles à l'adresse:http://ec.europa.eu/newsroom/document.cfm?doc id=44137
[6] https://edps.europa.eu/data-protection/our-work/our-work-bY-tvpe/guidelines_en
[7] Certaines grandes IUE ont des CPD qui font office d'interlocuteurs locaux dans chaque direction générale (ou autre unité analogue).
[8] Article 3, paragraphes 1 à 8, du règlement.

Cette boîte à outils n'aborde *pas* les sujets suivants:

- le rôle des DPD en général,
- les modalités exactes de gestion de certaines opérations de traitement particulières, telles que les transferts de données à caractère personnel en dehors de l'UE ou des processus spécifiques, comme la sélection et le recrutement de personnel[9].

Cette boîte à outils vous fournira des conseils sur la façon de gérer les risques liés à la protection des données et à la vie privée pour un processus opérationnel mené dans votre organisation et vous indiquera comment documenter ces activités. Pour des propositions de mesures spécifiques à mettre en œuvre, par exemple dans les procédures de sélection, veuillez vous reporter aux lignes directrices dédiées aux différentes opérations de traitement.

3 Le processus de responsabilisation

La responsabilité signifie qu'il incombe au responsable du traitement d'assurer la conformité et qu'il doit être en mesure de la démontrer. Dans la pratique, **la direction est responsable de la conformité avec les règles, mais la compétence est généralement assumée à un niveau inférieur** (propriétaire du processus). Le propriétaire de processus/la personne compétente pour le compte du responsable du traitement[10] chargé d'un processus sera aux commandes, assisté(e) par le DPD et les CPD (Partie I – section 2, Partie II – section 2).

Pour la plupart des opérations de traitement réalisées dans votre organisation, la tenue de registres et l'exécution d'un contrôle de conformité seront suffisantes. Seules certaines opérations de traitement nécessiteront une AIPD. Et parmi ces dernières, quelques-unes à peine exigeront aussi une consultation préalable.

Démontrer votre conformité signifie documenter **la façon dont vous traitez les données à caractère personnel et pourquoi vous avez choisi de le faire comme vous le faites**. Vos **obligations en matière de documentation dépendent des risques** posés par la nature du traitement des données à caractère personnel. Ainsi, un service d'abonnement à un bulletin d'informations requerra beaucoup moins de documentation qu'une base de données de profilage des voyageurs à des fins d'évaluation des risques. La façon dont vous concevez vos processus influe également sur ces considérations. En effet, une évaluation du personnel reposant sur un simple entretien avec l'évaluateur nécessitera moins de documentation qu'un système qui génère automatiquement des mesures comparatives à partir d'un système de gestion de cas et les utilise comme intrants pour la procédure d'évaluation du personnel.

[9] Pour ces cas particuliers, et pour bien d'autres situations (enquêtes administratives, procédures disciplinaires, gestion des congés et des horaires flexibles, données médicales, etc.), le CEPD a rédigé des lignes directrices plus détaillées, que vous trouverez ici: httpsy/edps.europa.eu/data-protection/our-work/our-work-by-type/guidelines_en. Le CEPD mettra ces documents à jour afin de les adapter aux nouvelles règles.

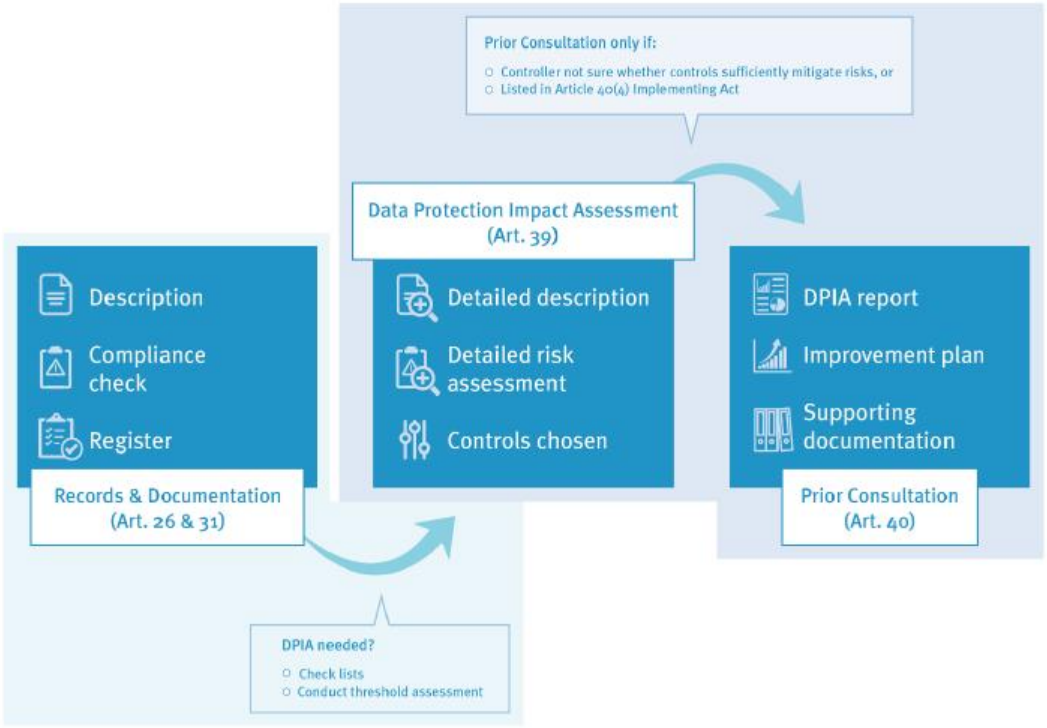
[10] Il peut arriver que le propriétaire d'un processus s'appuie sur les contributions d'autres parties. Exemple: le chef d'une unité pour laquelle le département informatique développe une application. Le propriétaire du processus sera peut-être amené à s'adresser au service informatique pour certaines questions, mais il n'en restera pas moins compétent pour le système dans son ensemble.

Contrôle de conformité et registres des activités de traitement (pour toutes les opérations de traitement)
AIPD (en cas de «risque élevé», liste du CEPD et actes d'exécution au titre de l'article 40, paragraphe 4)
Consultation préalable (en cas de «risque résiduel élevé» et actes d'exécution au titre de l'article 40, paragraphe 4)

Selon le processus concerné, vous n'aurez peut-être pas à suivre toutes les étapes ci-dessous:

- générer une documentation de base (appelée «registres») pour tous les processus; profiter de cette occasion pour aussi effectuer un contrôle de conformité,
- vérifier si le traitement est susceptible de présenter des risques élevés pour les personnes dont vous traitez les données et consulter le DPD si tel semble être le cas,
- si une AIPD est nécessaire, analyser les risques plus en détail et élaborer des garanties/mesures de maîtrise spécifiques pour les gérer,
- s'il ressort de l'AIPD que les risques résiduels restent élevés, consulter le CEPD.

Les deux premières étapes sont abordées dans la partie I de la présente boîte à outils, les deux dernières dans sa partie II.



4 Qu'entend-on par «registres»? [Partie I – section 3]

Vous devez tenir une documentation élémentaire pour toutes vos opérations de traitement. Cette documentation est appelée «registre». Le **règlement fournit une liste des éléments** à inclure dans les registres [Partie I – Section 3.1]. Lorsque vous créez un registre, vous devez également **vérifier si votre traitement est conforme** aux règles [Partie I – Section 3.2]. Reportez-vous à la [Partie I – Annexe 1] pour un modèle que vous pourrez utiliser dans ce contexte. Pour créer ces registres, vous

pouvez vous appuyer sur les notifications déjà existantes dans votre IUE [Partie I – Section 5]. Une fois ces registres créés, assurez-vous de bien les tenir à jour [Partie I – Section 3.3].

Ces registres alimentent un **registre central** tenu par votre IUE et géré par le DPD [Partie I – Section 3.4]. Le DPD est le mieux placé pour être le gardien de ce registre, mais, en tant que propriétaire de processus, vous restez compétent pour le contenu des registres que vous avez générés. **Certaines informations contenues dans ce registre doivent être publiques** [Partie I – Section 3.5].

Il s'agit de la documentation de protection des données requise pour la plupart des opérations de traitement.

5 Quand procéder à une analyse d'impact relative à la protection des données? [Partie I – Section 4]

Cela étant, certaines **opérations de traitement «à risque» doivent faire l'objet d'une vigilance accrue**. Cela concerne **par exemple** le traitement **de grands volumes** de **données à caractère personnel sensibles**, telles que des données relatives à la santé, à des questions disciplinaires ou l'utilisation de techniques de **profilage**, pour ne citer que quelques exemples. Il y a deux questions que vous devriez vous poser afin de déterminer si vous devez effectuer une AIPD.

- Cette opération figure-t-elle sur la liste établie par le CEPD en vertu de l'article 39, paragraphe 4, du règlement?
- L'analyse de seuil confirme-t-elle la nécessité d'une AIPD?

Si la réponse à l'une de ces questions est «oui», procédez à une AIPD. Le CEPD vous propose un **modèle** à utiliser pour cette analyse du seuil. En outre, il a adopté une liste au titre de l'article 39, paragraphe 4, du règlement, qui répertorie les critères à appliquer, et une liste indicative de certains «suspects habituels» à risque [partie II – annexe 5].

6 Comment procéder à une analyse d'impact relative à la protection des données? [Partie II – Section 3]

En vertu du règlement, vous devez effectuer des **AIPD pour les opérations de traitement susceptibles d'engendrer des «risques élevés»** pour les personnes dont vous traitez les données.

Le CEPD n'**impose pas de méthode spécifique** pour ce faire, mais il **fournit des modèles** sur lesquels vous pouvez vous baser pour effectuer des AIPD [Partie II – Annexe 3]. Si vous ne souhaitez pas utiliser ces modèles, vous pouvez avoir recours à toute autre méthode conforme aux prescriptions du règlement [vous trouverez une liste non exhaustive dans la Partie II – Annexe 4.1].

L'AIPD permet d'analyser plus en détail les opérations de traitement que vous envisagez afin de déterminer où se trouvent les risques liés à la vie privée et comment vous pouvez les atténuer. **Cela va plus loin que la gestion des risques de sécurité de l'information**. Dès que vous aurez réalisé cette analyse pour la première fois, vous disposerez d'un rapport d'AIPD expliquant votre traitement, les risques recensés et les mesures de maîtrise mises en œuvre (ou à mettre en œuvre). **Les AIPD sont un processus continu**, et non un exercice ponctuel – réexaminez-les à chaque changement majeur de vos opérations de traitement et, dans tous les cas, à intervalles réguliers afin de les tenir à jour [Partie II – Section 3.8].

Il est de **bonne pratique de publier vos rapports d'AIPD, à tous le moins sous la forme d'une synthèse**. Cette publication permet de mettre en avant le travail accompli pour rendre les opérations de traitement conformes et peut favoriser la confiance de vos parties prenantes et du grand public [Partie II – Section 3.9].

7 Quand procéder à une consultation préalable? [Partie II – Section 4]

Dans un rapport d'AIPD, trois résultats sont possibles:

(1) Vous êtes convaincu(e) que les mesures de maîtrise des risques retenues dans l'AIPD sont suffisantes pour ramener les risques à un niveau acceptable. Dans ce cas, mettez-les en œuvre et poursuivez le projet.
(2) Vous concluez que les mesures analysées ne peuvent pas ramener les risques à un niveau acceptable. Dans ce cas, vous devriez abandonner le projet ou le revoir de fond en comble puisqu'il se révèle impossible à mettre en œuvre de manière conforme.
(3) Vous ne savez pas avec certitude si les mesures de maîtrise des risques que vous avez analysées et sélectionnées sont suffisantes pour ramener les risques à un niveau acceptable.

Dans ce troisième cas, vous devez procéder à une «consultation préalable» du CEPD (article 40 du règlement). La Commission européenne peut également adopter des **actes d'exécution énumérant des types d'opérations de traitement qui nécessitent toujours une consultation préalable**.

Vous devrez remettre votre AIPD et d'autres informations au CEPD [Partie II – Section 4]. Le **CEPD répondra dans un délai de huit semaines**. Il pourra toutefois prolonger ce délai de quatre semaines supplémentaires pour les cas extrêmement complexes. Si nous avons besoin de plus amples informations de votre part, les demandes que nous adressons à ce sujet suspendent le délai. Dans sa réponse, le CEPD formulera des **recommandations visant à améliorer la conformité**, le cas échéant.

8 Comment se préparer? [Partie I – Section 5; Partie II – Section 5]

Votre IUE dispose déjà d'une certaine documentation sur la protection des données, **il n'est donc pas nécessaire de partir de zéro**. Pour générer des registres, vous pouvez **vous appuyer, pour commencer, sur les notifications envoyées à votre DPD en vertu de l'ancien règlement** (CE) 45/2001 [Partie I – Section 5]. Si vos notifications sont à jour, leur conversion en registres ne devrait pas demander trop de travail. Pour ce qui est des opérations de traitement présentant un risque plus élevé qui nécessitent une AIPD, nombre d'entre elles auront fait l'objet d'un «contrôle préalable» en vertu de l'ancien règlement [Partie II – Section 5].

D'autres changements se feront également jour avec le nouveau règlement. Ainsi, vous devrez surveiller de plus près vos **sous-traitants**[11] et devrez très probablement mettre à jour vos avis de protection des données[12].

9 Que peut faire votre DPD pour vous?

Chaque IUE compte au moins un délégué à la protection des données (DPD), qui sert de **point de référence pour toutes les questions liées à la protection des données**. Certaines grandes IUE ont également des contacts/coordinateurs de la protection des données (CPD) dans chaque direction générale. Ceux-ci peuvent vous fournir des conseils sur la façon de générer des registres et d'effectuer des AIPD. N'hésitez pas à les contacter si vous avez des questions sur la protection des données. Ne perdez cependant pas de vue que la conformité relève de la mission du responsable du traitement.

---

[11] Voir Consultation concernant certaines clauses qu'un sous-traitant souhaite inclure dans les contrats de service afin de les aligner sur les conditions énoncées par le règlement (UE) 2016/679https://edps.europa.eu/data-protection/our-work/publications/consultations/consultation-concerning-updating-service_en (en anglais). Des clauses types à utiliser dans ces contrats ont été distribuées aux DPD.

[12] Lignes directrices du CEPD concernant les articles 14 à 16 du nouveau règlement 45/2001: droits et obligations en matière de transparence, disponibles à l'adresse: https://edps.europa.eu/data-protection/our-work/publications/other-documents/articles-14-16-new-regulation-452001_en.

Les DPD font également office **d'interface entre les IUE et le CEPD**. À chaque fois que vous souhaitez poser une question au CEPD, veuillez la transmettre à votre DPD. Dans de nombreux cas, celui-ci connaîtra déjà la réponse.

10 Que peut faire le CEPD pour vous?

Le **CEPD est l'autorité de contrôle du traitement des données à caractère personnel par les IUE**.
À ce titre, nous surveillons et vérifions le respect des règles de protection des données, que ce soit en réponse à des plaintes, lors d'inspections, en réponse à des consultations envoyées par des institutions européennes ou de notre propre initiative. Nous fournissons des conseils en matière de conformité, en nous appuyant sur notre expérience, et proposons des formations pour vous aider à devenir un chef de file en matière de protection des données et à mettre en œuvre les meilleures pratiques.

Outre ce rôle de surveillance, le CEPD agit également **en tant que conseiller du législateur de l'UE** concernant les nouvelles règles relatives au traitement des données à caractère personnel, telles que les propositions d'actes juridiques établissant de nouvelles bases de données de l'UE. Nous assurons également le **secrétariat du Comité européen de la protection des données**, forum dans l'enceinte duquel les autorités européennes de protection des données coopèrent sur des questions transfrontalières.