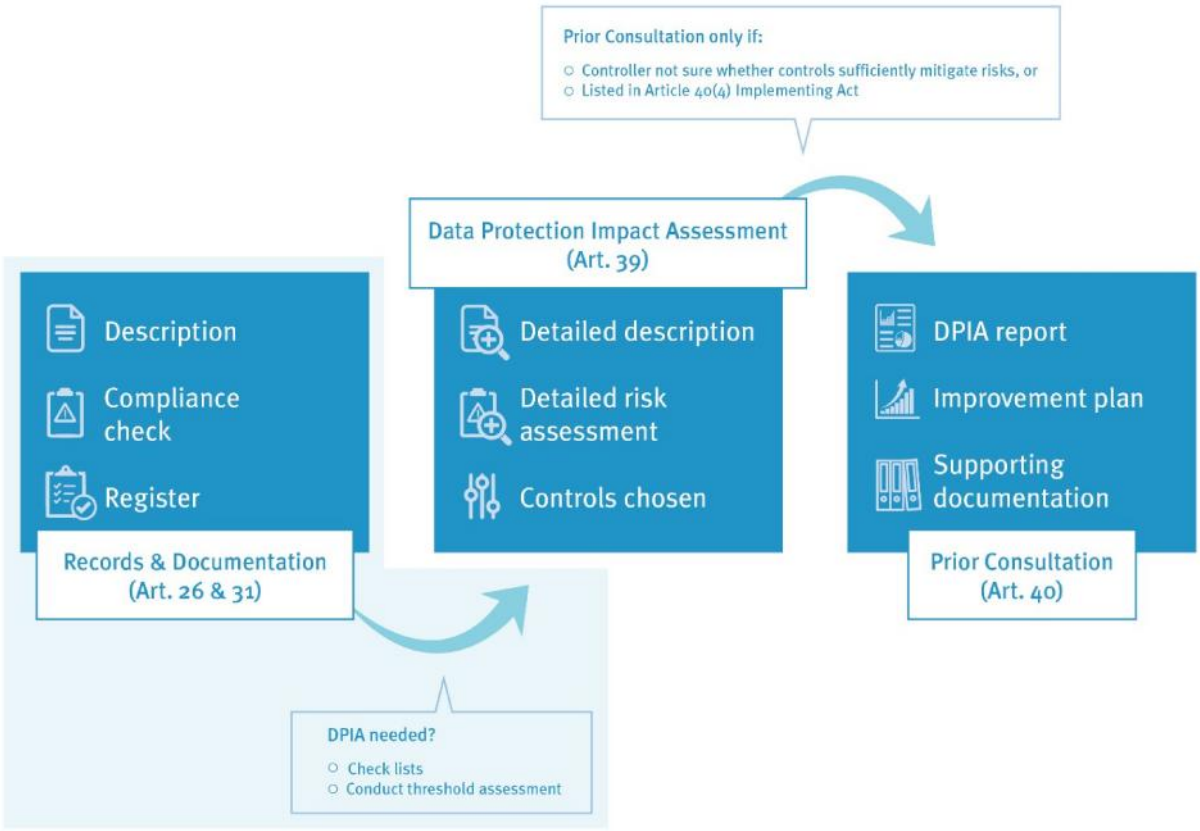
LE CONTRÔLEUR EUROPÉEN DE LA PROTECTION DES DONNÉES (CEPD)

Responsabilisation sur le terrain – Partie I: registres, registres centraux et quand procéder à une analyse d'impact relative à la protection des données

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	Description
Compliance check	Contrôle de conformité
Register	Registre central
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

Table des matières

Table des figures

1. Partie I: introduction et domaine d'application

En tant que propriétaire d'un processus/personne compétente pour le compte du responsable du traitement, vous devez créer des «registres» par processus [article 31 du règlement (UE) 2018/1725 – ci-après le «règlement»[1]] des opérations de traitement des données à caractère personnel effectuées dans votre IUE. Cela signifie que vous devrez, par exemple, créer un «registre» pour les procédures de sélection et de recrutement, et un autre pour les procédures de lutte contre le harcèlement.

La partie I de la présente boîte à outils vous montre comment générer ces registres et la documentation connexe. Elle explique également comment décider s'il est nécessaire de réaliser une analyse d'impact relative à la protection des données (AIPD).

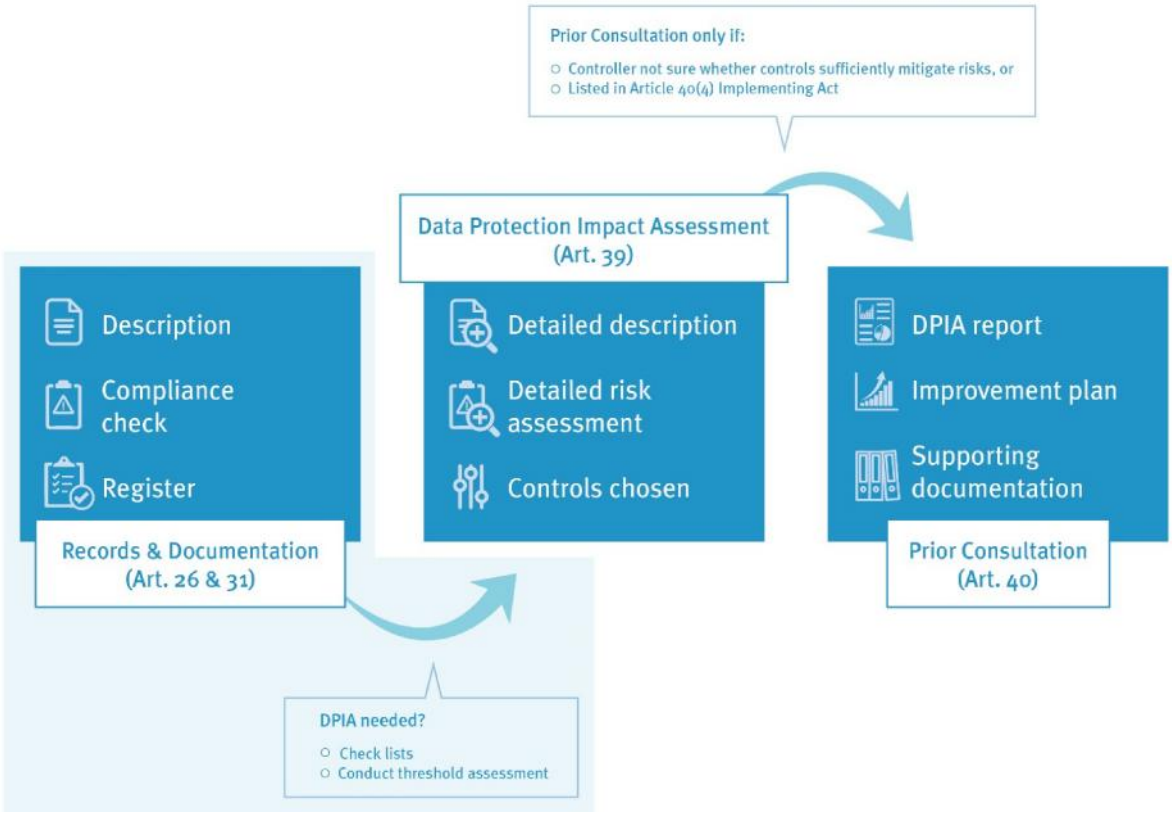


Figure 1: domaine d'application de la partie I

La présente partie fournit des orientations sur la manière de se conformer au règlement lors de l'élaboration de nouveaux processus opérationnels («activités de traitement» dans la terminologie de la protection des données) et sur la manière de gérer la documentation requise en matière de protection des données. Elle couvre les aspects suivants et fournit des modèles pour la plupart d'entre eux:

- comment documenter vos activités de traitement,
- qui fait quoi dans ce contexte,
- comment évaluer si vous devez effectuer une AIPD,
- les règles de transition depuis l'ancien règlement sur la protection des données applicables aux institutions de l'UE en ce qui concerne les registres.

[1] JO L 295 du 21.11.2018, p. 39.

Pour les questions suivantes, veuillez plutôt vous reporter à la partie II:

- comment réaliser des AIPD,
- quand envoyer une AIPD au CEPD pour consultation préalable.

2. Responsabilités et compétences – qui fait quoi?

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 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»[2]. Dans la pratique, **la direction est responsable de la conformité avec les règles, mais la compétence est généralement assumée à un niveau inférieur** («personne compétente pour le compte du responsable du traitement» / «responsable du traitement dans la pratique»). Dans de nombreux cas, le propriétaire du processus sera aussi la personne compétente. **En tant que propriétaire d'un processus, vous en serez la cheville ouvrière et serez assisté(e) dans votre tâche par le DPD** (et les CPD, le cas échéant)[3].

Il incombe au responsable du traitement de tenir des registres appropriés (en pratique: la direction en assume la responsabilité, et le propriétaire du processus la compétence)[4]. Le CEPD recommande vivement aux institutions européennes de centraliser leurs registres dans un **registre public tenu par le DPD**[5]. Cela n'affecte en rien la responsabilité du responsable du traitement des données concernant la génération des registres et leur contenu. Bien que le DPD puisse vous apporter son aide dans la génération des registres et de la documentation connexe, cette tâche reste la vôtre. De même, c'est à vous qu'il appartient, en tant que propriétaire du processus, de vérifier si vous devez procéder à une AIPD. Votre DPD peut vous y aider, mais c'est à vous de vous en charger.

La matrice RACI[6] ci-dessous donne un aperçu des différents rôles[7] dans le domaine des registres. Veuillez noter qu'il s'agit d'un aperçu général. Selon les opérations de traitement concernées, vous devrez peut-être y associer d'autres équipes, telles que l'unité/le service juridique de votre IUE.

	Compétent	Responsable	Consulté	Informé
Direction		**X**		
Propriétaire du processus	**X**			
DPD			**X**	

[2] Article 3, paragraphes 1 à 8, du nouveau règlement

[3] 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.

[4] Articles 26 et 31 du règlement.

[5] Voir aussi les sections 3.3 et 3.5 ci-dessous.

[6] «compétent, responsable, consulté, informé» – cadre pour l'attribution des tâches et des responsabilités.

[7] «Compétent» signifie avoir l'obligation d'agir et de prendre des décisions pour atteindre les résultats attendus; «responsable» signifie être comptable des actions, des décisions et du rendement; «consulté» signifie être invité à apporter sa contribution et à fournir des commentaires; «informé» signifie être tenu informé des décisions prises et du processus.

Service informatique			**X**	
Sous-traitants, le cas échéant			**X**	

Figure 2: matrice RACI du processus registres/documentation

La direction est responsable du respect des règles en matière de protection des données. Cependant, dans la pratique, l'essentiel du travail sera très vraisemblablement accompli par les propriétaires de processus spécifiques. Étant donné que le propriétaire du processus peut s'appuyer sur d'autres parties, internes (par exemple, le service informatique) et externes (par exemple, des sous-traitants ou fournisseurs d'informations), ces dernières doivent être consultées et, si nécessaire, fournir un retour. Dans la plupart des cas, votre service informatique fournira l'infrastructure technique et sera le mieux placé pour apporter son concours aux aspects de sécurité de l'information.

Enfin, vous devriez consulter votre DPD tout au long du processus, car il est le principal pôle de connaissances de votre IUE en matière de protection des données. **Votre DPD peut faire œuvre de facilitateur, mais gardez bien à l'esprit qu'en dernière analyse, la compétence et la responsabilité incombent au responsable du traitement des données**. Les DPD doivent aider les responsables du traitement à faire leur travail, et non le faire à leur place. Veuillez vous reporter à l'annexe 1 pour un résumé des rôles au cours des différentes étapes abordées dans cette partie de la boîte à outils.

3. Documentation de vos opérations de traitement

3.1 Qu'entend-on par «registres»?

Documentez vos opérations de traitement à l'aide de «registres». Concernant les opérations de traitement héritées pour lesquelles vous avez déjà reçu des notifications «article 25» en vertu de l'ancien règlement, vous pouvez utiliser celles-ci comme base pour vos registres.

En tant que personne compétente pour le compte du responsable du traitement, **vous êtes tenu(e) de générer des registres pour toutes vos activités de traitement portant sur des données à caractère personnel** – des bulletins d'information de votre IUE à vos tâches métier, en passant par la sélection du personnel, les enquêtes administratives et les procédures disciplinaires. Ces registres contiennent des informations de base sur les opérations de traitement telles que «Qui est responsable? Quelles sont les finalités du traitement? Quelles données traitons-nous à propos de quelles personnes?» Ils constituent la base de votre documentation en matière de protection des données et sont l'une des premières choses que le CEPD examinera lors de l'évaluation de votre conformité aux règles de protection des données.

Même si un nouveau projet n'est pas encore suffisamment avancé pour commencer à créer un registre, **c'est toujours une bonne idée d'en parler à votre DPD**: plus tôt vous prendrez conscience des aspects problématiques des opérations de traitement prévues, plus il sera facile de corriger le tir.

Les registres ne sont pas une nouveauté: l'article 25 de l'ancien règlement (CE) 45/2001 prévoyait déjà la présentation au DPD de notifications avec un contenu analogue. Vous pouvez réutiliser celles-ci pour générer vos registres. Les informations contenues dans les registres sont très proches de celles que vous devez inclure dans les avis de protection des

données/déclarations de confidentialité informant les personnes de vos opérations de traitement. Vous pouvez **réutiliser le texte** des uns dans les autres.

L'article 31 du nouveau règlement vous fournit une liste d'informations à inclure dans les registres:

a) les noms et coordonnées du responsable du traitement (y compris les responsables conjoints, le cas échéant), du DPD et des éventuels sous-traitants (le cas échéant);
Qui est responsable? À qui s'adresser? Utilisez des boîtes aux lettres fonctionnelles, et non les boîtes aux lettres personnelles du propriétaire du processus et du DPD (c'est préférable pour la continuité de l'activité et plus facile à mettre à jour)[8]*. Au final, c'est le rôle dans l'organisation qui compte, et non la personne qui occupe actuellement ce rôle. Si vous avez recours à un sous-traitant pour traiter des données à caractère personnel, mentionnez-le (par exemple, services informatiques externalisés ou contrôles médicaux préalables à l'embauche); si vous êtes responsable conjointement avec une autre IUE ou une autre organisation, dites-le (par exemple, deux IUE partageant un même service médical).*

b) les finalités du traitement;
Pourquoi faites-vous cela? Fournissez une description très concise de ce que vous avez l'intention de réaliser avec le traitement des données à caractère personnel; si vous vous appuyez sur une base juridique spécifique, mentionnez-la également (par exemple, le statut du personnel pour les procédures RH, missions assignées à votre IUE par le droit de l'Union).

c) une description des catégories de personnes concernées et des données qui seront traitées à leur sujet;

Qui est concerné? Quelles informations conservez-vous à leur sujet? Dans l'hypothèse où les catégories de données diffèrent selon les catégories de personnes, expliquez (par exemple suspects et témoins dans le cadre d'une enquête).

d) les catégories de destinataires auxquels des données peuvent être communiquées;

Qui aura accès à ces informations (en interne et à l'externe)? Qui a accès à quelles parties des données? Remarque: il n'est pas nécessaire de mentionner les entités qui ne peuvent avoir accès aux données que dans le cadre d'une mission d'enquête particulière (par exemple, l'OLAF, le Médiateur européen, le CEPD)[9]*.*

e) les transferts vers des destinataires situés dans des pays tiers ou des organisations internationales, avec mention du pays tiers/de l'organisation internationale concerné(e) et documentation des garanties appropriées pour ce transfert;

Si vous communiquez des données à de telles parties, qui sont-elles et comment vous assurez-vous qu'elles les traitent équitablement (par exemple un sous-traitant dans un pays tiers utilisant des clauses contractuelles types)?

[8] Si l'article 31 du règlement parle ici du «nom» du DPD, les articles 15 et 16 (sur les informations à fournir aux personnes concernées) ne font référence qu'à ses coordonnées. Le CEPD est d'avis qu'il n'est pas nécessaire ici de fournir le nom de la personne physique qui remplit actuellement le rôle de DPD dans une IUE – ce qui importe, c'est que les personnes concernées aient un point de contact au sein de l'organisation.
[9] Voir l'article 3, paragraphe 1, point 13), du règlement; pour plus d'informations sur les règles équivalentes du RGPD, veuillez consulter le considérant 31 du RGPD.

f) les délais prévus pour l'effacement des différentes catégories de données;

Pendant combien de temps conservez-vous les informations, et à partir de quand? Indiquez votre délai de conservation administratif, ainsi que son point de départ; établissez une distinction entre les catégories de données ou les catégories de personnes, le cas échéant (par exemple, dans les procédures de sélection: les candidats inscrits sur la liste de réserve par rapport à ceux qui ne l'ont pas été).

g) dans la mesure du possible, une description générale des mesures de sécurité adoptées.

Que pouvez-vous dire de la façon dont vous protégez les données traitées? Cela ne signifie pas divulguer le détail de vos mesures de sécurité de l'information, mais en donner une description générale qui ne porte pas atteinte à leur efficacité.

La première partie du **modèle de formule proposé à l'annexe 2** contient ces points, des instructions pour les remplir et un exemple de registre. Seule cette première partie, qui contient les **informations énumérées à l'article 31 du nouveau règlement, relève de l'obligation de publication** examinée à la section 3.5 ci-dessous.

3.2 Contrôle de la conformité et des risques

Profitez de la génération de vos registres pour vérifier que vos opérations de traitement sont conformes aux règles de protection des données. Vous devez vous conformer aux règles et être en mesure de le prouver.

La création des registres est un **bon moment pour vérifier le respect** des règles de protection des données, dont doivent rendre compte les responsables du traitement. Les responsables du traitement doivent concevoir les processus de manière à s'assurer qu'ils sont conformes aux règles (voir l'article 4, paragraphe 2, et l'article 26 du règlement).

La deuxième partie du formulaire figurant à l'annexe 2 contient une **courte liste de contrôle** relative aux règles principales. Vous devez vous conformer au règlement et être en mesure de démontrer cette conformité, en tenant compte des risques engendrés par les opérations de transformation (article 26 et considérant 38 du règlement). Cette **attitude proactive face au risque** est l'un des grands changements par rapport aux anciennes règles: pensez toujours à la façon dont le traitement pourrait affecter les personnes dont vous traitez les données. Quelles sont les répercussions pour elles? Comment cela les affecte-t-il? Si les choses se passent comme prévu et en cas de problème. Cette liste de contrôle peut vous servir d'outil pour mener cette réflexion. Bien que ne faisant pas partie du registre stricto sensu, elle montre que vous avez pensé aux implications du traitement en matière de protection des données.

Il y a deux aspects fondamentaux ici: «ce traitement est-il licite?» et «respectons-nous les principes en matière de protection des données?» Le modèle proposé à l'annexe 2 est assorti d'explications concernant la façon de le remplir et vous trouverez d'autres informations juridiques à l'annexe 3. Vérifier et documenter ces aspects de conformité au moment où vous créez vos registres vous aide à respecter les règles et à le prouver («responsabilité» à l'article 4, paragraphe 2)[10]. Pour les aspects «sécurité de l'information» de la conformité en matière de

[10] Logiquement, le contrôle de conformité précède le registre: si vous vous rendez compte que vous ne pouvez pas effectuer certaines opérations de traitement de manière licite, vous devriez abandonner le projet, de sorte que le registre ne sera pas nécessaire. Dans la pratique, il peut être judicieux de faire passer le registre avant le contrôle de conformité: la lisibilité de vos opérations est plus grande si vous décrivez d'abord ce que vous faites (ou

protection des données, assurez-vous de disposer d'un processus de gestion des risques de sécurité de l'information adéquat et choisissez des mesures de maîtrise appropriées en fonction des risques engendrés par les opérations de traitement[11].

À la fin du contrôle de conformité, vous trouverez également quelques questions de filtrage pour vous aider à déterminer si vos opérations de traitement peuvent présenter des «risques élevés» et nécessitent donc une analyse plus approfondie. Si vous cochez l'une de ces cases, parlez-en à votre DPD; il se peut que vous deviez effectuer une AIPD. Pour plus d'informations sur les AIPD, veuillez vous reporter à la partie II de la présente boîte à outils.

3.3 Réexamen des registres

Veillez à ce que les registres reflètent toujours la réalité des opérations de traitement auxquelles ils se rapportent.

Vos registres doivent refléter la réalité des opérations de traitement de votre IUE. Vous devez **vous assurer qu'ils sont à jour**. Lorsque vous prévoyez des changements dans vos opérations de traitement, vérifiez si le registre doit être mis à jour. **Il est judicieux d'inclure ce contrôle formellement dans votre processus de gestion du changement**. Il peut également être intéressant de procéder régulièrement à un réexamen de vos registres, indépendamment des changements prévus, afin de repérer les modifications qui auraient pu passer inaperçues.

3.4 Tenue d'un registre central

Votre IUE doit tenir ces registres par écrit (y compris sous forme électronique – article 31, paragraphe 3, du règlement) et les mettre à la disposition du CEPD sur demande (article 31, paragraphe 4). Conformément à l'article 31, paragraphe 5, «[p]our autant que ce soit approprié compte tenu de la taille de l'institution ou de l'organe de l'Union, les institutions et organes de l'Union consignent leurs activités de traitement dans un registre central».

Le CEPD recommande vivement que toutes les IUE tiennent un registre central des opérations de traitement et que celui-ci soit géré par le DPD.

En vertu de l'ancien règlement, les IUE tenaient un registre central. Il est tout à fait judicieux, pour des raisons pratiques, de poursuivre cette pratique.

- Un tel registre permet d'obtenir facilement une vue d'ensemble des activités de traitement de votre organisation, de manière à pouvoir maîtriser ses opérations.
- Il permet de répondre plus facilement aux demandes relatives aux registres, qu'elles émanent du CEPD ou d'autres parties prenantes.
- Il facilite la comparaison de vos registres, ce qui rend plus aisé le contrôle de la qualité de ceux-ci.
- Il aide votre DPD à mener à bien sa mission qui consiste à garantir l'application du règlement à l'interne.

prévoyez de faire) et ensuite pourquoi vous le faites de cette façon et comment vous vous assurez de la conformité aux règles applicables.

[11] Pour plus de détails, veuillez consulter les lignes directrices du CEPD sur les mesures de sécurité concernant le traitement des données à caractère personnel (https://edps.europa.eu/data-protection/our-work/publications/guidelines/security-measures-personal-data-processing_en, en anglais) et le cadre de gestion des risques de sécurité de l'information de votre IUE.

- Il vous permet de voir plus aisément comment d'autres opérations de traitement analogues ont été documentées dans votre organisation, facilitant ainsi la génération de registres.

Le CEPD recommande que ce soient les DPD des IUE qui tiennent ces registres, pour les raisons suivantes:

- Les DPD sont des pôles de connaissances en matière de protection des données – ils sont votre premier interlocuteur lorsque vous vous demandez comment vous conformer aux règles de protection des données. Disposer de tous les registres permettra au DPD de mieux répondre à vos questions éventuelles.
- Les DPD peuvent ainsi avoir une vue d'ensemble des activités de traitement des organisations, ce qui les aide à fournir de meilleurs conseils (par exemple sur la façon dont d'autres pans de l'organisation gèrent des questions analogues).
- Le registre visé à l'article 25 de l'ancien règlement 45/2001, qui était l'équivalent fonctionnel du registre prévu à l'article 31, paragraphe 5, du règlement, était tenu par le DPD. Le maintien de cette pratique réduit la nécessité de changements organisationnels.

Veuillez toutefois noter **que même si le DPD *tient* le registre central, c'est l'IUE, en tant que responsable du traitement (et par extension, vous, en tant que personne compétente pour le compte du responsable du traitement), qui reste responsable du *contenu* des registres**.

En vertu des anciennes règles, nous recommandions que les DPD tiennent un «inventaire» des opérations de traitement prévues qui n'étaient pas suffisamment avancées dans leur planification pour faire l'objet d'une «notification au titre de l'article 25» (l'ancêtre des registres). Nous réitérons cette recommandation, car un tel «inventaire» peut se révéler être un précieux outil de planification.

3.5 Publicité des registres

Les registres constituent un outil important pour vérifier et que votre organisation a la maîtrise de ses activités de traitement et pour le documenter. Conformément à l'article 31, paragraphe 5, du règlement, les IUE mettent leurs registres à la disposition du public.

Les IUE sont tenues de rendre publics les registres relevant de l'article 31, de préférence par voie de publication sur l'internet, conformément à la pratique de nombreuses IUE en matière de notifications au titre de l'article 25 de l'ancien règlement.

Cette publication présente de nombreux avantages:

- elle contribue à la transparence des IUE[12],
- elle contribue à renforcer la confiance du public,
- elle facilite le partage des connaissances entre les IUE.

Veuillez noter que ces exigences de publication ne s'appliquent qu'aux registres relevant de l'article 31 à proprement parler (c'est-à-dire aux éléments énumérés à l'article 31, paragraphe 1, du nouveau règlement) et non aux autres documents que votre IUE peut détenir. Le modèle fourni à l'annexe 2 est divisé en plusieurs parties, ce qui facilite la publication des seules informations visées à l'article 31.

[12] Voir également l'article 15, paragraphe 1, du TFUE.

4. Quand effectuer une AIPD?

4.1 Critères pour établir l'obligation d'effectuer une AIPD

Vous n'aurez pas à réaliser d'AIPD pour toutes les opérations de traitement. Seules celles susceptibles de présenter un «risque élevé pour les droits et la liberté des personnes concernées» nécessitent une AIPD. Il vous incombe, en tant que personne compétente pour le compte du responsable du traitement, de préparer l'AIPD. Vous serez pour cela assisté(e) et guidé(e) par le DPD.

Vous devez effectuer une AIPD lorsque votre opération répond à au moins l'un des critères ci-dessous:

(1) elle figure sur la liste des types d'opérations de traitement à risque que le CEPD est appelé à publier;
(2) elle est susceptible d'engendrer des risques élevés d'après votre analyse de seuil.

Le nouveau règlement prévoit plusieurs listes non exhaustives d'opérations de traitement nécessitant une AIPD et une évaluation de votre part pour les cas qui ne figurent pas dans ces listes. Pour savoir si les opérations de traitement que vous prévoyez nécessitent une AIPD, posez-vous les questions suivantes:

1. Est-elle répertoriée dans une liste établie par le CEPD en vertu de l'article 39, paragraphe 4? Dans l'affirmative, effectuez une AIPD.
2. Est-elle répertoriée dans une liste établie par le CEPD en vertu de l'article 39, paragraphe 5? Dans l'affirmative, vérifiez qu'elle relève bien des points mentionnés et que vous n'aurez pas à effectuer une AIPD.
3. Si elle ne figure dans aucune des listes, effectuez une analyse de seuil pour savoir si vous devez effectuer une AIPD.

Conformément à l'article 39 du règlement (soulignement ajouté).

> *«1. Lorsqu'un type de traitement, en particulier par le recours à de nouvelles technologies, et compte tenu de la nature, de la portée, du contexte et des finalités du traitement, est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, le responsable du traitement effectue, avant le traitement, une analyse de l'impact des opérations de traitement envisagées sur la protection des données à caractère personnel. Une seule et même analyse peut porter sur un ensemble d'opérations de traitement similaires qui présentent des risques élevés similaires.*
>
> […]
>
> *(3) L'analyse d'impact relative à la protection des données visée au paragraphe 1 est, en particulier, requise dans les cas suivants:*
>
> > *(a) l'évaluation systématique et approfondie d'aspects personnels concernant des personnes physiques qui est fondée sur un traitement automatisé, y compris le profilage, et sur la base de laquelle sont prises des décisions produisant des effets juridiques à l'égard d'une personne physique ou l'affectant de manière significative de façon similaire;*

(b) le traitement à grande échelle de catégories particulières de données visées à l'article 10, ou de données à caractère personnel relatives à des condamnations pénales et à des infractions visées à l'article 11; ou

(c) la surveillance systématique à grande échelle d'une zone accessible au public.»

Cette liste est **non exhaustive**, comme l'indique l'utilisation des mots «en particulier». D'autres opérations de traitement peuvent franchir le seuil du «risque élevé pour les droits et libertés des personnes physiques». Pour les AIPD en vertu du RGPD, le GT29 a fourni des orientations, approuvées depuis par le Comité européen de la protection des données. Celles-ci comprennent entre autres des critères portant sur les opérations de traitement soumises à une AIPD en vertu du RGPD[13]. **L'analyse de seuil vous aide à déterminer si les opérations de traitement prévues atteignent ce seuil.**

Conformément au paragraphe 4 du même article, **le CEPD établit et publie une liste des «types d'opérations de traitement» pour lesquelles une AIPD est requise**. Le CEPD peut également établir une liste négative des types d'opérations de traitement non soumises à une AIPD, conformément au paragraphe 5 du même article. Le CEPD a adopté cette liste le 16 juillet 2019. Elle est reproduite à l'annexe 5 du présent document.

En vertu de l'article 40, paragraphe 4, du règlement, la Commission européenne peut adopter des actes d'exécution qui répertorient des types d'opérations de traitement nécessitant une consultation préalable. Pour que le CEPD puisse y répondre, il vous faudra effectuer une AIPD avant. Si la Commission européenne devait arrêter de tels actes d'exécution, **nous ajouterions les opérations de traitement visées à notre liste publiée au titre de l'article 39, paragraphe 4**. Vous ne devrez ainsi vérifier qu'une seule liste.

Si vous concluez qu'une AIPD est nécessaire, veuillez vous reporter à la partie II de la présente *boîte à outils sur la responsabilisation*.

L'article 39, paragraphe 9, du règlement introduit une **dérogation** à l'obligation de procéder à une AIPD. Cet article précise que, pour les opérations de traitement ayant 1) une base juridique spécifique réglementant l'opération de traitement spécifique ou l'ensemble d'opérations en question et pour lesquelles 2) une AIPD a déjà été effectuée dans le cadre d'une analyse d'impact générale pour la base juridique proposée, aucune AIPD n'est nécessaire. Pour être considérées comme une AIPD au sens du règlement, ces analyses doivent être beaucoup plus détaillées que les analyses d'impact actuellement envisagées pour les propositions législatives. Pour faire simple, les analyses d'impact actuelles du processus législatif de l'UE s'attachent à répondre à la question «cette proposition est-elle judicieuse?»[14], tandis que les AIPD des IUE s'interrogent sur «comment pouvons-nous remplir cette tâche qui nous a été confiée d'une manière conforme et respectueuse de la vie privée?».

Par ailleurs, même lorsqu'une AIPD a été réalisée dans le respect des normes du règlement au stade de la proposition de base juridique, un réexamen serait très vraisemblablement nécessaire avant le lancement des opérations. La raison en est que la base juridique adoptée est susceptible de différer de la proposition d'une manière affectant les questions liées à la protection de la vie privée et à la protection des données. En outre, il n'est généralement pas vrai que tous les choix opérés dès la conception ayant une incidence sur la vie privée et la protection des données soient

[13] Voir http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236.

[14] Pour obtenir de l'aide pour répondre à cette question s'agissant des aspects relatifs à la protection des données, veuillez consulter la boîte à outils sur la nécessité du CEPD.

déjà déterminés par la base juridique. **Dans la pratique, de telles AIPD prévues dans le cadre du processus législatif peuvent *tout au plus* constituer la première étape du processus de l'AIPD.**

4.2 Listes positives/négatives du CEPD

Si le type d'opération de traitement que vous souhaitez mettre en œuvre figure dans la liste positive du CEPD au titre de l'article 39, paragraphe 4, du règlement, effectuez une AIPD.

Veuillez vous reporter à l'annexe 5 pour les listes adoptées au titre de l'article 39, paragraphes 4 et 5, du règlement. Les exemples fournis ne sont pas exhaustifs.

Conformément à l'article 40, paragraphe 4, du nouveau règlement, la Commission européenne peut adopter des actes d'exécution exigeant une consultation préalable pour des cas spécifiques d'opérations de traitement effectuées dans le cadre d'une mission d'intérêt public exercée par un responsable du traitement, y compris le traitement de telles données dans le cadre de la protection sociale et de la santé publique. Ces actes d'exécution s'appliqueront à toutes les institutions de l'UE, et pas seulement à la Commission européenne elle-même.

Pour que le CEPD puisse répondre à ces consultations préalables (voir aussi section 4 de la partie II), il vous faudra effectuer une AIPD avant. La Commission européenne n'a à ce jour pas adopté de tels actes d'exécution. **Si la Commission européenne devait le faire, nous inclurions ces types d'opérations de traitement dans notre liste au titre de l'article 39, paragraphe 4**, afin d'en faciliter la consultation.

4.3 Analyse de seuil

S'agissant des opérations de traitement qui ne figurent pas dans la liste des AIPD obligatoires, mais que le DPD de votre IUE et/ou vous soupçonnez néanmoins d'être à haut risque, effectuez une analyse de seuil à l'aide du modèle fourni à l'annexe 5. De manière générale, vous devriez effectuer une AIPD si vous avez coché au moins deux critères. Documentez cette analyse de seuil.

Si les opérations de traitement que vous prévoyez ne figurent dans aucune des deux listes et que vous ne savez pas avec certitude si une AIPD est nécessaire, consultez votre DPD et effectuez une analyse de seuil. **L'annexe 5 contient un modèle** pour la réalisation de cette analyse de seuil.

Ce modèle **est basé sur les critères des «types d'opérations de traitement à risque» publiés par le GT29[15] et approuvés par le Comité européen de la protection des données**, avec quelques adaptations au contexte spécifique des IUE. Ainsi, le statut du personnel explique déjà comment fonctionne l'évaluation du personnel dans l'IUE, ce qui réduit à la fois la marge de manœuvre du responsable du traitement pour son organisation et la vulnérabilité du personnel (par exemple, les mécanismes de recours sont déjà juridiquement définis).

Le modèle demande si le traitement concerné présente certaines caractéristiques – par exemple, un but d'exclure des personnes d'un droit, d'une prestation ou d'un contrat, ou d'inclure le traitement de catégories spéciales de données, telles que des données sur la santé. Si c'est le

[15] Voir note 13 ci-dessus.

cas, expliquez comment et pourquoi exactement; dans les cas limites, vous devez également décrire pourquoi vous ne considérez pas que le critère est rempli. Les critères vont au-delà de la liste indicative de l'article 39, paragraphe 3, sur la base de l'interprétation par le GT29 de règles équivalentes dans le RGPD. **De manière générale, vous devriez effectuer une AIPD si vous avez coché au moins deux critères**.

Toutefois, l'évaluation ne saurait être réduite à un simple calcul du nombre de critères remplis. La décision n'est pas automatique. En effet, dans certains cas, un traitement répondant à un seul de ces critères peut nécessiter une AIPD. Et dans d'autres, une AIPD peut ne pas être nécessaire alors que le traitement remplit deux critères, voire plus. **Si vous cochez deux critères ou plus et ne considérez pas que le traitement entraînerait des risques élevés pour les personnes concernées, expliquez pourquoi après avoir consulté le DPD de votre IUE**.

5. Comment se préparer?

Le suivi de vos opérations de traitement n'est pas une obligation nouvelle. En vertu de l'article 25 de l'ancien règlement, vous deviez, en tant que personne compétente pour le compte du responsable du traitement, notifier à votre DPD tous les traitements concernant des données à caractère personnel. Votre DPD les consignait alors dans un registre accessible au public.

Commencez par vous appuyer sur vos notifications existantes au titre de l'article 25 de l'ancien règlement pour créer vos registres. Générez des registres pour les nouvelles opérations de traitement à mesure que vous les développez.

Ces notifications peuvent servir de base pour générer des registres (voir l'annexe 4 pour un tableau des correspondances). Pour les opérations de traitement existantes, transformez vos notifications existantes au titre de l'article 25 en registres. Si vos notifications sont à jour, leur conversion en registres ne devrait pas demander trop de travail. Pour les nouvelles opérations de traitement, générez des registres à mesure que vous les développez.

Le **règlement ne prévoyait pas de période de transition en dehors des vingt jours habituels suivant sa publication au Journal officiel de l'UE**. Transformez vos notifications au titre de l'article 25 en registres au plus vite.

Si vous devez établir des priorités, commencez par les registres au titre de l'article 31 pour les opérations de traitement les plus risquées. Le contrôle de conformité est un outil qui vous aidera à fournir des preuves quant aux raisons qui vous ont poussé(e) à traiter les données comme vous le faites.

6. Conclusion

La partie I de la *boîte à outils sur la responsabilisation* vous a fourni des conseils pratiques sur la façon de générer des registres de vos opérations de traitement et de savoir si vous deviez effectuer une AIPD. Dans de nombreux cas, vous n'aurez besoin que du registre.

En tant que personne compétente pour le compte du responsable du traitement/propriétaire du processus, **c'est vous qui êtes aux commandes** – la conformité à la protection des données relève de votre responsabilité. Votre DPD sera votre guide, mais c'est à vous qu'il appartiendra de sélectionner et de mettre en œuvre les mesures concrètes en vue d'assurer la conformité.

Les registres sont le fondement de votre documentation en matière de protection des données. La non-tenue de registres peut valoir une amende administrative à votre IUE[16]. Lorsque le CEPD vérifiera que votre IUE respecte ses obligations en matière de protection des données, vous pouvez être sûr(e) qu'il examinera vos registres. De même, s'il y a une violation de données dans votre IUE et que vous devez en informer le CEPD[17], celui-ci vous demandera le ou les registres concernés.

Vous n'aurez pas à créer des registres à partir de zéro, mais vous pourrez commencer en vous appuyant sur les notifications déjà faites en vertu de l'ancien règlement. Efforcez-vous de les mettre rapidement à jour, car les registres sont la base de votre documentation en matière de protection des données.

Les registres ne sont pas une fin en soi, mais un outil pour montrer que vous avez réfléchi à la conformité avec les règles en matière de protection des données dès la conception de vos opérations de traitement.

Certaines opérations de traitement plus risquées nécessitent une analyse supplémentaire. Si vous concluez que vos opérations de traitement requièrent une AIPD, faites-la. Selon le résultat de l'AIPD, vous devrez peut-être également procéder à une «consultation préalable» du CEPD. Pour plus d'orientations concernant les AIPD, veuillez vous reporter à la partie II de la présente boîte à outils.

[16] Article 66 du règlement; un projet de document d'orientation a été envoyé aux DPD pour information.
[17] Article 37 du règlement; les lignes directrices du CEPD sur la notification de violation de données sont disponibles ici: https://edps.europa.eu/data-protection/our-work/publications/guidelines/guidelines-personal-data-breach-notification_en.

Annexes

1 Qui fait quoi?

La liste ci-dessous donne un aperçu des différents rôles, en définissant les tâches respectives des responsables du traitement/propriétaires de processus et des DPD.

Responsable du traitement/propriétaire de processus:

- créer des projets de registres,
- répondre aux questions de contrôle de la conformité,
- vérifier si vous devez effectuer une AIPD,

DPD:

- fournir un retour sur les projets de registres et d'autres documents,
- tenir un registre central,
- répondre aux consultations des responsables du traitement/propriétaires de processus,
- assurer l'interface entre l'IUE et le CEPD.

Autres fonctions (telles que les services informatiques ou juridiques)

- venir en aide au responsable du traitement/propriétaire de processus et au DPD au besoin.

2 Registres et liste de contrôle en matière de conformité

En vertu de l'article 31 du nouveau règlement, les IUE doivent tenir des registres de leurs opérations de traitement. Le présent modèle couvre deux aspects:

1. registres obligatoires au titre de l'article 31 des nouvelles règles (recommandation: accessibles au public)
2. contrôle de conformité et détection des risques (en interne).

L'en-tête et la partie 1 devraient être accessibles au public; la partie 2 est interne à l'IUE. À titre d'exemple, la colonne 3 contient un registre hypothétique concernant les badges et le contrôle d'accès physique dans une IUE.

Nº	**Point**	**Explication**	**Exemple: contrôle d'accès**
	En-tête – numéros de version et de référence (recommandation: accessibles au public)		
1.	Dernière mise à jour de ce registre		25/05/2018
2.	Numéro de référence	Pour le suivi; si votre IUE tient un registre central, contactez le détenteur de ce registre pour obtenir un numéro de référence.	IUE/Logistique/1.1
	Partie 1 - Registre au titre de l'article 31 (obligation légale spécifique de publication – voir l'article 31, paragraphe 5)		
3.	Nom et coordonnées du responsable du traitement	Utilisez autant que possible des boîtes aux lettres fonctionnelles, et non personnelles. Cela permettra de gagner du temps lors de la mise à jour des registres et contribuera à la continuité de l'activité.	Responsable du traitement: IUE, Place de l'Europe 1, Ville, État membre Contact: Directeur de la logistique, IUE fmb-logistics@eui.europa.eu
4.	Nom et coordonnées du DPD	Ce champ sera prérempli.	DPD, IUE dpo@eui.europa.eu
5.	Nom et coordonnées du responsable du traitement conjoint (le cas échéant)	Si vous êtes responsable conjointement avec une autre IUE ou organisation, veuillez l'indiquer ici (par exemple, deux IUE qui se partagent un service médical). Si c'est le cas, assurez-vous de mentionner dans la description qui se charge de quoi et à qui les personnes peuvent adresser leurs requêtes.	Sans objet
6.	Nom et coordonnées du sous-traitant (le cas échéant)	Si vous avez recours à un sous-traitant pour traiter des données à caractère personnel pour votre compte, veuillez l'indiquer (par exemple, évaluations à 360°, services informatiques externalisés ou contrôles médicaux préalables à l'embauche).	Sans objet

Nº	Point	Explication	Exemple: contrôle d'accès
7.	Finalité du traitement	Description très concise de ce que vous avez l'intention de réaliser; si vous agissez en vous référant à une base juridique spécifique, mentionnez-le également (par exemple, le statut du personnel pour les procédures de sélection).	Assurer la sécurité physique dans les locaux de l'IUE en contrôlant l'accès aux bâtiments de l'IUE en général et aux zones sensibles à l'intérieur de ceux-ci (par exemple, les salles d'archives); compter les personnes présentes dans le bâtiment à des fins d'évacuation, conformément à la décision de l'IUE en matière de sécurité, articles X et Y.
8.	Description des catégories de personnes dont [l'IUE] traite les données et liste des catégories de données	Dans l'hypothèse où les catégories de données diffèrent selon les catégories de personnes, veuillez également fournir une explication (par exemple: suspects et témoins dans le cadre d'une enquête)	Nous traitons les données suivantes concernant chaque personne à qui un badge d'accès aux bâtiments de l'IUE a été délivré (c'est-à-dire le personnel et les sous-traitants sur site, à l'exclusion des visiteurs accompagnés):) nom et photo [imprimés sur le badge et gérés de manière centralisée],) lien avec l'IUE [personnel/sous-traitant, géré de manière centralisée],) numéro de badge [seule information stockée dans la balise RFID du badge],) portes/portiques pour lesquels le badge est valable [géré de manière centralisée];) date d'expiration du badge [imprimée sur le badge et gérée de manière centralisée];) lorsque le badge est présenté aux portes/portiques: horodatage, ID de la porte/du portique, numéro de badge [géré de manière centralisée].
9.	Délai de conservation des données	Indiquez votre délai de conservation administratif, ainsi que son point de départ; établissez une distinction entre les catégories de personnes ou de données, le cas échéant (par exemple, dans les procédures de sélection: les candidats inscrits sur la liste de réserve par rapport à ceux qui ne l'ont pas été).	Nous conservons les données pendant deux mois à compter de l'expiration/de la révocation du badge, à l'exception des journaux d'accès, que nous conservons pendant deux mois sur une base glissante.
10.	Destinataires des données	Qui, dans votre IUE, aura accès aux données? Qui aura accès aux données en dehors de votre IUE? Remarque: il n'est pas nécessaire de mentionner les entités qui ne peuvent avoir accès aux données que dans le cadre d'une	Agent de sécurité de l'IUE chargé du suivi des incidents de sécurité et des enquêtes. Les gardes n'ont accès qu'au nombre de personnes actuellement présentes dans le bâtiment (données agrégées,

Nº	Point	Explication	Exemple: contrôle d'accès
		mission d'enquête particulière (par exemple, l'OLAF, le Médiateur européen, le CEPD).	pas de données à caractère personnel).
11.	Y a-t-il des transferts de données à caractère personnel à des pays tiers ou à des organisations internationales? Dans l'affirmative, lesquels et avec quelles garanties?	Par exemple, un sous-traitant dans un pays tiers utilisant des clauses contractuelles types, une autorité publique de pays tiers avec laquelle vous coopérez sur la base d'un traité. Si nécessaire, consultez votre DPD pour plus d'informations sur la façon de mettre en place des garanties.	Non
12.	Description générale des mesures de sécurité, si possible.	Incluez une description générale de vos mesures de sécurité, que vous pourriez également fournir au grand public.	Nous conservons les données sur les détenteurs de badges et les journaux d'accès électroniquement dans des systèmes à accès limité sécurisés par les pratiques de sécurité standard de l'IUE, conformes à notre système de gestion de la sécurité de l'information certifié ISO 27001. La seule information stockée électroniquement (balise RFID) sur le badge est le numéro de badge. Elle ne peut pas être lue à plus de 5 cm.
13.	Pour plus d'informations, y compris sur la manière d'exercer vos droits d'accès, de rectification, d'opposition et de portabilité des données (le cas échéant), reportez-vous à la déclaration de confidentialité:	Bien que la publication de la déclaration de confidentialité ne fasse pas partie du registre stricto sensu, cela accroît la transparence et n'ajoute aucune charge administrative, puisqu'elle existe déjà.	[lien vers la politique de confidentialité]
	Partie 2 – contrôle de conformité et détection des risques (en interne)		
	Contrôle de conformité (articles 4 et 5)		
14.	Base juridique et nécessité du traitement (voir article 5 du nouveau règlement): (a) nécessaires à l'accomplissement de missions d'intérêt public dont l'IUE est investie par le droit de l'Union (a2) a) conformément au	Cochez (au moins) une case et expliquez en quoi le traitement est nécessaire. Exemples: (a) une mission dont votre IUE est investie par la législation, par exemple des procédures en vertu du statut du personnel ou des missions assignées à une agence par son règlement fondateur. Veuillez mentionner la base juridique spécifique (par exemple, «article X du statut du personnel, tel que mis en œuvre par l'article Y du RI de l'IUE», plutôt que simplement	(a2) pas spécifiquement mentionné dans le droit primaire ou dérivé de l'UE, mais requis pour la sûreté et la sécurité du personnel, des bâtiments et des informations. Voir également la décision de l'IUE sur la sécurité 2017/XXXX, articles X et Y.

Nº	Point	Explication	Exemple: contrôle d'accès
	considérant 17, deuxième phrase (b) nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis (c) nécessaire à l'exécution d'un contrat auquel la personne concernée est partie; ou (d) consentement (e) intérêt vital	«statut du personnel»); (a2) toutes les opérations de traitement nécessaires au fonctionnement des IUE ne sont pas explicitement prescrites par la législation; le considérant 17 explique qu'elles sont néanmoins couvertes ici, par exemple l'annuaire interne du personnel, le contrôle d'accès; (b) une obligation légale spécifique de traiter les données à caractère personnel, par exemple l'obligation de publier des déclarations d'intérêt prévue par le règlement fondateur d'une agence de l'UE; (c) cela concerne rarement les IUE; (d) si les personnes ont donné leur consentement libre et éclairé, par exemple utilisation d'un photomaton lors de la journée portes ouvertes de l'UE, publication facultative de photos dans le répertoire interne; (e) par exemple, le traitement d'informations sur la santé par le service de secours de première ligne après un accident lorsque la personne ne peut pas donner son consentement.	
15.	Définition des finalités	Énumérez-vous toutes les finalités au point 7 ci-dessus? Les finalités sont-elles spécifiées, explicites, légitimes? Lorsque des informations sont également traitées à d'autres fins, êtes-vous sûr(e) que celles-ci ne sont pas incompatibles avec la ou les finalités initiales?	Oui. Vérifier que seules les personnes autorisées accèdent aux bâtiments de l'IUE sert à assurer la sûreté et la sécurité de notre personnel, des informations et d'autres actifs. Nous utilisons également des journaux d'accès pour connaître le nombre de personnes actuellement présentes dans le bâtiment (à des fins d'évacuation). Les journaux peuvent également, au cas par cas, être utilisés pour enquêter sur les incidents (par exemple «qui est entré dans la salle des archives pendant la période où des fichiers ont disparu?») conformément aux procédures applicables (voir le registre IUE-123.4 sur les enquêtes administratives), ce qui ne semble pas incompatible. Nous en informons les détenteurs de badge lors de la

Nº	Point	Explication	Exemple: contrôle d'accès
			délivrance du badge (voir la déclaration de confidentialité).
16.	Minimisation des données	Avez-vous vraiment besoin de toutes les données que vous prévoyez de collecter? Y en a-t-il dont vous pourriez vous passer?	La photo, le nom et la date d'expiration du badge sont nécessaires pour les contrôles visuels effectués par les agents de sécurité; le numéro de badge est nécessaire pour gérer les droits d'accès aux zones réglementées et les révocations. Il est nécessaire de tenir des registres d'accès (qui, quand, où) pour enquêter sur des incidents tels que des vols ou la disparition de documents.
17.	Exactitude	Comment vous assurez-vous que les informations que vous traitez à propos des personnes sont exactes? Comment rectifiez-vous les informations inexactes?	Le nom et la photo sont recueillis directement auprès de la personne qui demande un badge. Les pointeuses aux portiques d'accès sont synchronisées. Les détenteurs d'un badge peuvent demander que leur nom et leur photo soient modifiés.
18.	Limitation de la conservation	Expliquez pourquoi vous avez choisi le ou les délais de conservation mentionnés au point 9 ci-dessus. Sont-ils limités selon la maxime «aussi long que nécessaire, aussi court que possible»? Dans l'hypothèse où vous n'auriez besoin que de certaines informations sur une période plus longue, pouvez-vous scinder les délais de conservation?	Un délai de deux mois pour les journaux d'accès constitue un juste équilibre entre le fait de pouvoir encore enquêter sur les incidents (qui peuvent ne pas être détectés immédiatement, par exemple un vol pendant une période de vacances) et le fait de ne pas conserver les journaux trop longtemps. Les informations relatives aux détenteurs d'un badge doivent être conservées pendant la durée de validité du badge. Le fait de les conserver pendant deux mois après l'expiration/la révocation nous permet d'encore enquêter sur des incidents susceptibles d'impliquer des membres du personnel partis récemment (sinon, nous ne pourrions pas savoir à qui un badge expiré se rapportait).
19.	Transparence: Comment informez-vous les personnes sur le traitement?	Par exemple, déclarations de confidentialité sur les formulaires, notifications par courrier électronique; si vous ne souhaitez pas informer les personnes (ou seulement a posteriori), consultez votre DPD!	Déclaration de confidentialité sur le formulaire de demande de badge et courte notice d'information au dos du badge avec un lien vers la déclaration de confidentialité publiée.
20.	Accès et autres droits des personnes dont vous traitez les données	Comment les personnes peuvent-elles vous contacter si elles veulent savoir quelles données vous avez à leur sujet, les corriger ou les supprimer, demander leur verrouillage ou s'opposer à leur traitement? Comment réagirez-vous? Si vous	Voir la déclaration de confidentialité: envoyez un courrier électronique à l'adresse logistics@eui.europa.eu, nous répondrons conformément aux délais et procédures standard définies dans les règles de mise en œuvre de la protection des

Nº	Point	Explication	Exemple: contrôle d'accès
		pensez qu'il pourrait y avoir des situations où vous pourriez vouloir refuser, par exemple, de leur permettre d'y accéder, parlez-en à votre DPD.	données de l'IUE (décision de l'IUE 2018/1234, section Y).
	Détermination des risques élevés		
21.	Ce traitement concerne-t-il un ou plusieurs des éléments suivants? J données relatives à la santé, aux infractions pénales (présumées) ou considérées comme sensibles pour d'autres raisons («catégories de données spéciales»), J évaluation, prise de décision automatisée ou profilage, J surveillance des personnes concernées, J nouvelles technologies qui peuvent être considérées comme intrusives.	Certaines opérations de traitement à risque nécessitent des garanties et une documentation supplémentaires. Si vous avez coché l'un de ces éléments, parlez-en à votre DPD pour plus d'informations et de conseils.	Non
	Partie 3 – Documentation connexe (interne)		
22.	(le cas échéant) liens avec l'analyse de seuil et l'AIPD	Si vous avez effectué une analyse de seuil et/ou une AIPD, faites-y référence ici	s.o.
23.	Où sont documentées vos mesures de sécurité de l'information?	Les règles de l'IUE en matière de sécurité de l'information vous obligent très probablement à documenter vos mesures de sécurité; une sécurité appropriée de l'information est également une exigence en matière de protection des données. Veuillez indiquer un lien vers la documentation pertinente en matière de sécurité de l'information.	[lien vers la documentation InfoSec]
24.	Autres documents connexes	Veuillez fournir des liens vers d'autres documents de ce processus (p. ex. documentation du projet, manuels)	[Lien vers le concept de sécurité physique pour l'IUE]

3 Explications supplémentaires sur les registres/modèles de contrôle de conformité

Le modèle figurant à l'annexe 1 contient déjà quelques explications sur la façon de le remplir. Dans la présente annexe, vous trouverez d'autres informations sur le contexte juridique. Nous aborderons ici deux grands volets: «ce traitement est-il licite?» et «respectons-nous les principes en matière de protection des données?»

Article 5 – Licéité du traitement

Concernant la première question, le traitement doit répondre à l'une des conditions énoncées à l'article 5 du règlement. Il s'agit de la question «pourquoi sommes-nous autorisés à faire cela?»:

«Article 5 – Licéité du traitement

1. *Le traitement n'est licite que si, et dans la mesure où, au moins une des conditions suivantes est remplie:*
   a) *le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi l'institution ou l'organe de l'Union;*
   b) *le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis;*
   c) *le traitement est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci;*
   d) *la personne concernée a consenti au traitement de ses données à caractère personnel pour une ou plusieurs finalités spécifiques;*
   e) *le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique.*
2. *Le fondement du traitement visé au paragraphe 1, points a) et b), est inscrit dans le droit de l'Union.»*

Dans la plupart des cas, vous vous fonderez sur le **point a)**. Cela concerne entre autres les missions que le droit de l'UE confie à votre institution – qu'il s'agisse des missions spécifiques de votre IUE ou de règles administratives relatives, par exemple, à la gestion du personnel ou aux marchés publics conformément au statut du personnel et au règlement financier. Ces bases juridiques spécifiques peuvent également fournir des instructions supplémentaires sur certains aspects du traitement (catégories de données, délais de conservation, etc.).

Conformément au considérant 22, deuxième phrase, du règlement, le point a) «comprend le traitement de données à caractère personnel nécessaire pour la gestion et le fonctionnement de ces institutions et organes», et par exemple pour tenir un annuaire interne du personnel. Ceci est mentionné au point a2) du formulaire.

Le **point b)** ne concerne que des obligations juridiques spécifiques de traitement des données à caractère personnel, par exemple la publication de déclarations d'intérêts spécifiquement prescrite dans les règlements fondateurs de certaines agences de l'UE[18].

[18] La limite entre les points a) et b) est qu'au point a), votre IUE se voit confier une mission dont l'exécution nécessite le traitement de données à caractère personnel (par exemple, l'évaluation du personnel), tandis qu'au point b), votre IUE a une obligation spécifique de traiter des données à caractère personnel clairement énoncées dans le droit de l'UE sans marge de manœuvre sur la manière de mettre ce traitement en œuvre (par exemple, «l'Agence prend des mesures pour prévenir et détecter les conflits d'intérêts» par rapport à «la déclaration d'intérêts du directeur exécutif est publiée»).

Le **point c)** fait référence au traitement nécessaire à l'exécution d'un contrat auquel la personne dont vous traitez les données est partie ou aux étapes préliminaires de la conclusion d'un tel contrat. Les IUE y ont rarement recours – un exemple issu du secteur privé serait la livraison de marchandises commandées par correspondance: le vendeur doit connaître l'adresse de livraison pour pouvoir remplir sa part du contrat (la conservation de cette adresse a posteriori peut toutefois ne pas être une nécessité).

Le **point d)** fait référence aux traitements auxquels les personnes ont consenti. Ce consentement doit être libre, éclairé et spécifique[19]. Les IUE n'utilisent pas souvent ce motif de licéité, car la grande majorité des données à caractère personnel qu'elles traitent relèvent du point a) ci-dessus. Parmi les cas où les IUE se fondent sur le consentement, citons l'exemple des abonnements à des bulletins d'information ou d'un photomaton mis à disposition lors d'une journée portes ouvertes de l'UE.

Le **point e)** concerne le traitement dans l'intérêt vital de la personne concernée ou d'une autre personne physique. Par exemple, les soins médicaux d'urgence dispensés par le service de secours de première ligne à la suite d'un accident du travail.

Dans certains cas, vous pouvez vous fonder sur plusieurs des points ci-dessus pour différents aspects du traitement. Par exemple, disposer d'un annuaire interne du personnel est «nécessaire pour la gestion et le fonctionnement» de votre IUE, mais pas avoir des photos du personnel dans celui-ci. Vous pouvez offrir la possibilité aux membres du personnel de télécharger des photos sur la base de leur consentement, mais vous ne pouvez pas les y forcer ou faire pression sur eux pour qu'ils le fassent.

Article 4 – Principes de protection des données

Les principes de protection des données énoncés à l'article 4 constituent le fondement des règles plus détaillées du nouveau règlement. Il s'agit de la question «Comment procédons-nous?»;

«Article 4 – Principes relatifs au traitement des données à caractère personnel

1. Les données à caractère personnel doivent être:

a) traitées de manière licite, loyale et transparente au regard de la personne concernée (licéité, loyauté, transparence);

b) collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités; le traitement ultérieur à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques n'est pas considéré, conformément à l'article 13, comme incompatible avec les finalités initiales (limitation des finalités);

c) adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (minimisation des données);

d) exactes et, si nécessaire, tenues à jour; toutes les mesures raisonnables doivent être prises pour que les données à caractère personnel qui sont inexactes, eu égard aux finalités pour lesquelles elles sont traitées, soient effacées ou rectifiées sans tarder (exactitude);

[19] Voir Groupe de travail «article 29», Avis 15/2011 sur la définition du consentement (WP 187).

e) conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées; les données à caractère personnel peuvent être conservées pour des durées plus longues dans la mesure où elles seront traitées exclusivement à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques conformément à l'article 13, pour autant que soient mises en œuvre les mesures techniques et organisationnelles appropriées requises par le présent règlement afin de garantir les droits et libertés de la personne concernée (limitation de la conservation);

f) traitées de façon à garantir une sécurité appropriée des données à caractère personnel, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées (intégrité et confidentialité).

2. Le responsable du traitement est responsable du respect du paragraphe 1 et est en mesure de démontrer que celui-ci est respecté (responsabilité).»

Pour chacun de ces points, demandez-vous comment votre IUE se conforme à ces exigences, en tenant compte de l'explication supplémentaire ci-dessous:

Le terme **«licite»** au point a) renvoie au contrôle de l'article 5 ci-dessus.

Le point a) fait également référence à la **«transparence»**, ce qui signifie que vous devez dire aux personnes que vous traitez leurs données à caractère personnel, pourquoi et comment (comme précisé plus en détail par les articles 14 à 16). Certaines restrictions sont possibles, pensez par exemple aux premières étapes d'une enquête de l'OLAF. Si vous collectez les données directement auprès des personnes concernées, par exemple via un questionnaire, fournissez-leur ces informations à ce moment-là. Si vous les recueillez ailleurs, pensez à la manière dont vous pouvez informer les personnes – la simple publication d'un avis de protection des données ne suffit généralement pas, car il peut ne pas nécessairement atteindre les personnes concernées. Pour plus d'informations, reportez-vous aux lignes directrices du CEPD sur les articles 14 à 16 du règlement[20], ainsi que sur l'article 25[21].

Un aspect de la notion de **«loyauté»** mentionnée au point a) réside dans le fait que les personnes dont vous traitez les données ont certains droits (tels que précisés aux articles 14 et 17 à 24 du nouveau règlement), par exemple celui de savoir quelles données vous conservez à leur sujet, de les faire corriger si nécessaire, de les faire supprimer si elles sont conservées de manière illicite, etc. Pour plus d'informations, voir les Lignes directrices sur les droits des individus concernant le traitement des données à caractère personnel[22]. Cela signifie également que vous devez concevoir vos systèmes et processus de manière à pouvoir répondre facilement à de telles requêtes.

La première partie du point b) est déjà couverte par le champ **«finalité»** du registre. Ce principe est également lié à la loyauté: vous devez définir clairement les objectifs afin que les personnes concernées sachent à quoi s'attendre. Cela nécessite que vous expliquiez clairement pourquoi votre IUE traite des données à caractère personnel. Les règles strictes concernant le traitement ultérieur visent à éviter des situations où, par exemple, des informations seraient réutilisées pour

[20] https://edps.europa.eu/sites/edp/files/publication/18-01-15_guidance_paper_arts_en_1.pdf

[21] Un projet de document d'orientation sur les règles internes au titre de l'article 25 du règlement a été envoyé aux DPD pour information.

[22] https://edps.europa.eu/data-protection/our-work/publications/guidelines/rights-individuals_en

exercer des représailles à l'encontre de lanceurs d'alerte. Veuillez noter que le nouveau règlement ne prévoit pas d'autorisation générale de tout conserver pendant une période prolongée à des fins d'archivage, de recherche scientifique, historiques ou statistiques. Le traitement doit dans chaque cas se fonder sur une base juridique appropriée et vous devez évaluer la nécessité et la proportionnalité de tout stockage de données. Vous devez en outre réfléchir aux garanties que vous pouvez mettre en place – par exemple, agréger les données à caractère personnel conservées/divulguées à des fins de recherche, interdire la réidentification dans les conditions d'octroi de l'accès à des fins de recherche, etc.

La **«minimisation des données»** visée au point c) signifie que vous devez être en mesure d'expliquer, pour chaque catégorie de données, en quoi celle-ci est nécessaire pour atteindre l'objectif du traitement. Demandez-vous: «Avons-nous vraiment besoin de cela pour atteindre notre objectif? Pourrions-nous nous passer de ces données?»[23].

L'**«exactitude»** au point d) signifie que vous devez consentir tous les efforts raisonnables pour vous assurer que les données que vous traitez sont exactes, car des décisions basées sur des informations erronées peuvent avoir des répercussions négatives sur les personnes et engager la responsabilité de votre IUE. Ce point est particulièrement important si vous ne collectez pas directement les données auprès des personnes qu'elles concernent, mais auprès d'autres sources. Dans certaines opérations de traitement, l'exactitude factuelle de déclarations peut être contestée par les parties concernées (pensez par exemple aux accusations d'un lanceur d'alerte). Dans de tels cas, l'«exactitude» fait référence au fait qu'une certaine déclaration (contenant des données à caractère personnel) a été faite et qu'elle a été correctement consignée; l'autre partie devrait pouvoir compléter les informations enregistrées et donner son propre point de vue sur la question[24].

Le principe de **«limitation de la conservation»** prévu au point e) signifie que, pour toute donnée à caractère personnel traitée, vous devez avoir une raison (liée à la finalité, voir ci-dessus) de la conserver aussi longtemps que vous le faites. Dans certains cas, la législation européenne applicable fixe des délais de conservation, mais dans d'autres, il appartient à votre IUE de les déterminer. Lorsque vous établissez ces délais, suivez la maxime «aussi long que nécessaire, aussi court que possible» en fonction de vos besoins opérationnels – les délais de conservation ne sont pas une question technique! Si des données doivent être conservées à des fins de preuve ou analogues, limitez l'accès à celles-ci aux profils d'utilisateurs spécifiques qui en ont besoin.

Enfin, le point f) indique que vous devez traiter les données à caractère personnel d'une manière qui assure une **«sécurité appropriée»**. Ce qui est «approprié» dépend des risques liés au traitement (voir aussi l'article 26). Cela inclut à la fois des mesures techniques et organisationnelles. Dans de nombreux cas, vous pourrez vous référer ici à votre documentation générale sur la gestion des risques de sécurité de l'information. Pour plus d'informations, voir

[23] Notez la différence par rapport à la nécessité du traitement dans son ensemble (lorsque vous expliquez l'article 5, point a), ci-dessus, la question qui se pose est: «après avoir établi que nous devons faire cela, *de quoi avons-nous besoin pour le faire*?»

[24] Pour donner un autre exemple: un membre du personnel n'est pas d'accord avec le feed-back négatif reçu de son supérieur hiérarchique lors d'une procédure d'évaluation. La déclaration du supérieur hiérarchique est «exacte» en ce sens qu'il s'agit de son évaluation. Néanmoins, l'agent devrait être en mesure de faire entendre son propre point de vue et de contester les rapports négatifs dans le cadre d'une procédure de recours. Si le rapport est modifié en appel, il ne s'agit toutefois pas d'une «rectification» au sens de l'article 14 du nouveau règlement.

les lignes directrices du CEPD sur les mesures de sécurité applicables au traitement des données à caractère personnel[25].

Le CEPD a fourni des documents d'orientation sur bon nombre de ces aspects[26]. Si nécessaire, le CEPD les actualisera à la lumière du nouveau règlement, une fois celui-ci adopté. Contactez votre DPD pour de plus amples informations.

4 Tableau de correspondances entre les notifications au titre de l'article 25 de l'ancien règlement et les registres prévus par le règlement

L'article 25 de l'ancien règlement énumérait les éléments obligatoires suivants pour les notifications au DPD:

(a) le nom et l'adresse du responsable du traitement et l'indication des services d'une institution ou d'un organe chargés du traitement de données à caractère personnel dans un but spécifique;
(b) la ou les finalités du traitement;
(c) une description de la catégorie ou des catégories de personnes concernées et des données ou des catégories de données s'y rapportant;
(d) la base juridique du traitement auquel les données sont destinées;
(e) les destinataires ou les catégories de destinataires auxquels les données sont susceptibles d'être communiquées;
(f) une indication générale des dates limites pour le verrouillage et l'effacement des différentes catégories de données;
(g) les transferts de données envisagés à destination de pays tiers ou d'organisations internationales;
(h) une description générale permettant une évaluation préliminaire du caractère approprié des mesures prises pour assurer la sécurité du traitement en application de l'article 22.

Les IUE utilisaient leurs propres modèles pour ces notifications, y ajoutant parfois des éléments supplémentaires, comme le fait de mentionner expressément si un sous-traitant était impliqué. L'article 31 du règlement, comme expliqué à la section 3.1 ci-dessus, répertorie les éléments obligatoires pour les registres générés au titre du règlement. La mise en correspondance de ces deux articles révèle leurs points communs et leurs différences. Comme vous le verrez, une grande partie des informations requises pour les registres est déjà disponible dans les anciennes notifications au titre de l'article 25. Vous pouvez vous appuyer sur ces informations pour créer vos registres.

Ancien article 25.	Article 31 du règlement.
(a)	(a), mais en ajoutant les coordonnées du DPD et, le cas échéant, du sous-traitant et/ou du responsable du traitement conjoint
(b)	(b)
(c)	(c)

[25] https://edps.europa.eu/data-protection/our-work/publications/guidelines/security-measures-personal-data-processing_en
[26] Voir https://edps.europa.eu/data-protection/our-work/our-work-by-type/guidelines_en

(d)	supprimé, mais mentionnez-le lors de la description des finalités visées au point b): dans la plupart des cas, le traitement par les IUE aura pour but d'accomplir les missions qui leur ont été assignées ou de se conformer aux obligations découlant de la législation de l'Union
(e)	(d), mais il est plus explicite que les destinataires dans les pays tiers/organisations internationales doivent également être mentionnés (mentionnez lesquels)
(g)	(e) ajoute des informations sur les garanties pour les transferts vers des pays tiers/organisations internationales (par exemple, clauses contractuelles types, décision d'adéquation, traité international)
(f)	(f) plus de mention spécifique du verrouillage; mentionnez vos délais de conservation ici (y compris la date de début)[27]
(h)	(g) il ne s'agit que d'une description générale des mesures prises.

[27] Cette information doit être incluse «dans la mesure du possible», mais conformément au principe de limitation de la conservation figurant à l'article 4, paragraphe 1, point e), votre IUE devrait toujours pouvoir donner un délai de conservation («X ans à compter de l'événement Y»). Si les données à caractère personnel sont publiées de manière licite et destinées à rester publiques sans limite de temps, mentionnez-les également.

5 Listes au titre de l'article 39, paragraphes 4 et 5, et modèle pour l'analyse de seuil

La décision du CEPD reproduite ci-dessous est [publiée sur le site web du CEPD](#).

EUROPEAN DATA PROTECTION SUPERVISOR

DÉCISION DU CONTRÔLEUR EUROPÉEN DE LA PROTECTION DES DONNÉES DU 16 JUILLET 2019 CONCERNANT LES LISTES D'AIPD PUBLIÉES AU TITRE DE L'ARTICLE 39, PARAGRAPHES 4 ET 5, DU RÈGLEMENT (UE) Nº 2018/1725

LE CONTRÔLEUR EUROPÉEN DE LA PROTECTION DES DONNÉES,

vu le règlement (UE) 2018/1725 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union et à la libre circulation de ces données, et abrogeant le règlement (CE) nº 45/2001 et la décision nº 1247/2002/CE[28], et notamment son article 39, paragraphes 4 et 5,

après consultation du Comité européen de la protection des données

attendu que:

(1) Les institutions, organes et agences de l'UE sont amenés à traiter d'importants volumes de données à caractère personnel concernant des personnes physiques, tant à l'intérieur qu'à l'extérieur des institutions. Ce traitement, même s'il est effectué de manière licite, peut entraîner des risques pour les droits et libertés de ces personnes. Les règles en matière de protection des données servent à garantir que les données à caractère personnel soient traitées de manière responsable, afin de réduire ces risques. Les obligations de documentation évoluent avec ces risques, les opérations de traitement «plus risquées» nécessitant une analyse plus approfondie.

(2) Les analyses d'impact relatives à la protection des données (AIPD) sont un concept nouveau introduit dans le règlement (UE) nº 2018/1725 (ci-après dénommé le «règlement»). Elles proposent un processus structuré pour gérer les risques en matière de protection des données posés par certaines opérations de traitement qui entraînent des «risques élevés» pour la personne concernée, et ne sont pas nécessaires pour tous les types d'opérations de traitement.

(3) Conformément à l'article 39, paragraphe 1, du règlement, «[l]orsqu'un type de traitement, en particulier par le recours à de nouvelles technologies, et compte tenu de la nature, de la portée, du contexte et des finalités du traitement, est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, le responsable du traitement effectue, avant le traitement, une analyse de l'impact des

[28] JO L 295 du 21.11.2018, p. 39 à 98.

opérations de traitement envisagées sur la protection des données à caractère personnel».

(4) Conformément à l'article 39, paragraphe 4, du règlement, le CEPD «établit et publie une liste des types d'opérations de traitement pour lesquelles une analyse d'impact relative à la protection des données est requise».

(5) Conformément à l'article 39, paragraphe 5, du règlement, le CEPD «peut aussi établir et publier une liste des types d'opérations de traitement pour lesquelles aucune analyse d'impact relative à la protection des données n'est requise».

(6) Conformément à l'article 39, paragraphe 6, du règlement, lorsque les listes visées à l'article 39, paragraphes 4 et 5, «ont trait à des opérations de traitement effectuées par un responsable du traitement agissant conjointement avec un ou plusieurs responsables du traitement autres que les institutions et organes de l'Union», le CEPD les soumet pour examen, avant adoption, au Comité européen de la protection des données, au titre de l'article 70, paragraphe 1, point e), du règlement (UE) nº 2016/679.

(7) Étant donné qu'il ne saurait y avoir aucune différence de traitement entre les situations dans lesquelles des institutions ou organes de l'Union sont seuls ou conjointement responsables du traitement des données et les situations dans lesquelles ils sont responsables du traitement conjointement avec une ou plusieurs entités autres que des institutions et organes de l'Union, le CEPD a décidé d'établir une liste unique pour l'article 39, paragraphe 4. Toutefois, la liste visée à l'article 39, paragraphe 5, ne couvre que des situations dans lesquelles des institutions ou organes de l'Union sont responsables du traitement, seuls ou conjointement, sans la participation de responsables autres, puisque les opérations de traitement qui y sont répertoriées se rapportent au traitement de données par les institutions ou organes de l'Union aux fins de leur gestion interne.

(8) Conformément au considérant 5 du règlement, «[c]haque fois que les dispositions du présent règlement suivent les mêmes principes que les dispositions du règlement (UE) 2016/679, ces deux ensembles de dispositions devraient […] être interprétés de manière homogène, notamment en raison du fait que le régime du présent règlement devrait être compris comme étant équivalent au régime du règlement (UE) 2016/679».

(9) Avant même que le règlement (UE) 2016/679 n'entre en vigueur, le groupe de travail «article 29» avait fourni des lignes directrices concernant l'article 35 dudit règlement[29], qui suit les mêmes principes que l'article 39 du règlement. Ces lignes directrices présentaient un ensemble de critères à utiliser afin d'établir l'existence possible d'un risque élevé. Lors de sa première réunion plénière, le Comité européen de la protection des données a approuvé les lignes directrices du GT29 relatives au RGPD[30].

(10) Ces lignes directrices confirmaient que les listes ne pouvaient prétendre être exhaustives, mais précisaient les critères permettant d'établir si un traitement est susceptible d'engendrer des risques élevés pour les personnes concernées. Les

---

[29] 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, wp248rev.01, adoptées le 4 avril 2017, telles que modifiées et adoptées en dernier lieu le 4 octobre 2017.

[30] Approbation du Comité européen de la protection des données 1/2018.

opérations de traitement spécifiques qui y sont mentionnées ne sont fournies qu'à titre d'exemple. Le fait qu'une opération de traitement particulière ne soit pas répertoriée à l'annexe 2 ne signifie pas qu'aucune AIPD ne soit nécessaire. À l'inverse, l'absence d'une opération donnée à l'annexe 3 ne veut pas non plus dire qu'elle ne doive pas faire l'objet d'une AIPD.

(11) En février 2018, le CEPD a publié des lignes directrices provisoires sur les obligations en matière de documentation[31] en vertu du règlement – non encore adopté à l'époque. Celles-ci comprenaient une première indication des types d'opérations de traitement susceptibles de nécessiter une AIPD, conformément aux lignes directrices publiées par le groupe de travail «article 29» et ultérieurement approuvées par le Comité européen de la protection des données. La présente liste s'appuie sur les orientations données aux responsables du traitement dans ce document.

(12) Le projet de liste a été soumis au Comité européen de la protection des données le 18 mars 2019, et une version mise à jour de celui-ci lui a été présentée le 21 juin 2019. Le Comité européen de la protection des données a rendu sa réponse le 10 juillet 2019[32]. La liste finale telle qu'adoptée tient compte de toutes les recommandations du comité.

(13) Il se peut que la Commission européenne adopte des actes d'exécution pour l'article 40, paragraphe 4, du règlement, établissant une liste de cas dans lesquels les responsables du traitement doivent consulter le CEPD et obtenir son autorisation préalable. Le responsable du traitement devrait également procéder à une AIPD dans ces cas, afin de permettre au CEPD de disposer d'une base solide pour trancher.

A ADOPTÉ LA PRÉSENTE DÉCISION:

Article premier

Objet et objectifs

1. La présente décision précise les circonstances dans lesquelles les responsables du traitement soumis au règlement (UE) 2018/1725 doivent effectuer une analyse d'impact relative à la protection des données (AIPD) en vertu de l'article 39 dudit règlement.
2. La présente décision s'applique sans préjudice des règles en matière d'analyses d'impact relatives à la protection des données et de consultation préalable définies aux articles 39 et 40 dudit règlement.

Article 2

Champ d'application et définitions

1. La présente décision s'applique à tous les responsables du traitement soumis au règlement (UE) 2018/1725.

[31] Accountability on the ground: Provisional guidance on documenting processing operations for EU institutions, bodies and agencies, version initiale publiée le 6 février 2018.
[32] Recommandation 01/2019 sur le projet de liste établi par le Contrôleur européen de la protection des données concernant les opérations de traitement pour lesquelles une analyse d'impact relative à la protection des données est requise [article 39, paragraphe 4, du règlement (UE) 2018/1725].

2. Les définitions figurant à l'article 3 du règlement (UE) 2018/1725 s'appliquent aux fins de la présente décision.

Article 3

Opérations de traitement nécessitant une AIPD (article 39, paragraphe 4, du règlement)

1. Lorsqu'il examine si les opérations de traitement prévues entraînent l'obligation de réaliser une AIPD en vertu de l'article 39 du règlement (UE) 2018/1725, le responsable du traitement utilise le modèle figurant à l'annexe 1 de la présente décision pour effectuer une analyse de seuil.
2. Si deux des critères du modèle figurant à l'annexe 1 au moins s'appliquent, le responsable du traitement procédera en règle générale à une AIPD.
3. Si le responsable du traitement décide de ne pas effectuer d'AIPD alors que plusieurs critères du modèle figurant à l'annexe 1 s'appliquent, il documente et motive cette décision.
4. Si les opérations de traitement prévues ne satisfont qu'à un seul critère du modèle figurant à l'annexe 1, le responsable du traitement peut néanmoins décider d'effectuer une AIPD.
5. L'annexe 2 de la présente décision recense plusieurs opérations de traitement courantes susceptibles de nécessiter une AIPD. Dans ces cas, le responsable du traitement n'est pas tenu de procéder à une analyse de seuil, mais effectue directement une AIPD.

Article 4

Opérations de traitement nécessitant une consultation préalable obligatoire [article 40, paragraphe 4, du règlement]

Si la Commission européenne adopte des actes d'exécution pour l'article 40, paragraphe 4, du règlement (UE) 2018/1725 contraignant les responsables du traitement à consulter le CEPD et à obtenir son autorisation préalable, les responsables du traitement effectuent également des AIPD pour les opérations de traitement répertoriées dans ces actes d'exécution.

Article 5

Opérations de traitement ne nécessitant pas d'AIPD [article 39, paragraphe 5, du règlement]

L'annexe 3 de la présente décision recense plusieurs opérations de traitement courantes qui, à première vue, ne nécessiteront vraisemblablement pas d'AIPD.

Article 6

Caractère non exhaustif des listes

Les listes des traitements annexées à la présente décision ne sont pas exhaustives.

Article 7

Entrée en vigueur

La présente décision entre en vigueur le jour suivant sa publication.

Pour le Contrôleur européen de la protection des données

[signé]
Wojciech Rafał WIEWIÓROWSKI

Annexe 1

Liste des critères permettant d'évaluer si des opérations de traitement sont susceptibles d'engendrer un risque élevé

En règle générale, si deux critères au moins de la liste s'appliquent, le responsable du traitement doit effectuer une AIPD. Si le responsable du traitement estime que, dans le cas d'espèce, les risques ne sont pas «élevés» en dépit de la présence de plusieurs «oui», il est tenu d'expliquer et de justifier pourquoi il estime que le traitement n'est pas «à risque élevé». Chaque critère est suivi de quelques exemples et contre-exemples de ce qui est susceptible (ou non) de le rendre pertinent.

I En-tête	
Nom de l'opération de traitement	[nom]
Point de contact pour le responsable du traitement	[fonction et coordonnées]
Registre des opérations de traitement	[référence du registre]
Consultation du DPD	[date du retour]
Approbation	[nom et date]
II Critères des traitements «susceptibles d'engendrer un risque élevé»	
Critère	Applicable? Oui [si oui, décrivez en quoi] / Non [si cas limite: pourquoi pas?]
1. Évaluation systématique et approfondie d'aspects personnels ou notation, y compris les activités de profilage et de prévision. *Exemples: une banque passant des transactions au crible, conformément à la législation applicable, en vue de détecter des transactions potentiellement frauduleuses; profilage du personnel en fonction de ses transactions dans un système de gestion de cas avec réaffectation automatique des tâches.* *Contre-exemples: entretiens d'évaluation standard, évaluations à 360° sur base volontaire pour aider le personnel à élaborer des plans de formation.*	[O (en quoi?) / N]
2. Prise de décisions automatisée avec effet juridique ou effet similaire significatif: traitement ayant pour finalité la prise de décisions à l'égard des personnes concernées. Exemple: évaluation automatisée du personnel («si vous êtes dans les 10 % inférieurs de l'équipe concernant le nombre de dossiers traités, vous recevrez une évaluation "insatisfaisant" sans autre forme de procès»). *Contre-exemple: un site d'actualités affichant des articles dans un ordre basé sur les visites passées de l'utilisateur.*	[O (en quoi?) / N]
3. Surveillance systématique: traitement utilisé pour observer, surveiller ou contrôler les personnes concernées, notamment dans les espaces accessibles au public. Cela peut concerner la vidéosurveillance, mais aussi d'autres activités de	[O (en quoi?) / N]

	surveillance, par exemple l'utilisation de l'internet par le personnel. *Exemples: vidéosurveillance secrète, vidéosurveillance intelligente dans des espaces accessibles au public, outils de prévention de la perte de données rompant le chiffrement SSL, suivi des mouvements via les données de localisation.* *Contre-exemple: vidéosurveillance annoncée à l'entrée d'un garage sans couverture de l'espace public.*	
4.	Données sensibles ou données à caractère hautement personnel: données révélant l'origine ethnique ou raciale, les opinions politiques, les convictions religieuses ou philosophiques, l'affiliation à un syndicat, données génétiques, données biométriques permettant d'identifier sans ambiguïté une personne physique, données relatives à la santé, à la vie sexuelle ou à l'orientation sexuelle, condamnations ou infractions pénales et mesures de sécurité connexes ou données à caractère hautement personnel. *Exemples: examens médicaux préalables au recrutement et vérifications du casier judiciaire, enquêtes administratives et procédures disciplinaires, tout recours à une identification biométrique 1:n.* *Contre-exemple: les photos ne sont pas sensibles en tant que telles (uniquement lorsqu'elles sont couplées à la reconnaissance faciale/biométrique ou utilisées pour déduire d'autres données sensibles).*	[O (en quoi?) / N]
5.	Données traitées à grande échelle, que ce soit en fonction du nombre de personnes concernées et/ou du volume de données traitées sur chacune d'elles et/ou de la permanence et/ou de la couverture géographique. *Exemple: bases de données européennes de surveillance épidémiologique.* *Contre-exemple: procédures d'invalidité au titre de l'article 78 du statut dans une IUE de taille moyenne.*	[O (en quoi?) / N]
6.	Croisement ou combinaison d'ensembles de données issus de plusieurs opérations de traitement de données différentes, effectuées à des fins différentes et/ou par différents responsables du traitement, d'une manière qui outrepasserait les attentes raisonnables de la personne concernée. *Exemples: recoupement des données de contrôle d'accès et des heures de travail auto-déclarées à la suite d'une suspicion de déclarations frauduleuses dans le cadre d'une enquête administrative (suivant les règles applicables).* *Contre-exemple: utilisation ultérieure de données traitées pour une demande de bourse lors d'un audit des procédures d'octroi des bourses.*	[O (en quoi?) / N]
7.	Données concernant des personnes vulnérables: situations dans lesquelles un déséquilibre des pouvoirs accru entre la personne concernée et le responsable du traitement peut être observé. *Exemples: enfants, demandeurs d'asile.* *Contre-exemples: délégués dans un groupe de travail du Conseil (pour les listes de présences), membres de groupes d'experts (pour le remboursement des frais de déplacement).*	[O (en quoi?) / N]
8.	Utilisation innovante ou application de solutions technologiques ou organisationnelles susceptibles d'impliquer de nouvelles formes de collecte et d'utilisation des données. En effet, les conséquences personnelles et sociales du déploiement d'une nouvelle technologie peuvent être inconnues. Exemples: apprentissage automatique, voitures connectées, sélection de candidats sur les réseaux sociaux. *Contre-exemple: contrôle d'accès biométrique 1:1 utilisant des empreintes digitales.*	[O (en quoi?) / N]

9. Traitements qui empêchent les personnes concernées d'exercer un droit ou de bénéficier d'un service ou d'un contrat. *Exemples: bases de données d'exclusion, sélection des emprunteurs.* *Contre-exemple: détermination des droits à la mise en service (par exemple, indemnité d'expatriation ou allocations familiales).*	[O (en quoi?) / N]
III Conclusion	
Nombre de «Oui» cochés ci-dessus	[n]
Évaluation: de manière générale, vous devriez effectuer une AIPD si vous avez coché au moins deux critères de la liste. Si vous estimez que, dans le cas d'espèce, les risques ne sont pas «élevés» en dépit de la présence de plusieurs «oui», expliquez et justifiez pourquoi vous pensez que le traitement n'est pas «à risque élevé».	[expliquez]

Annexe 2

Liste non exhaustive d'opérations de traitement courantes et indication de leurs risques a priori

Liste positive des opérations de traitement nécessitant à première vue une AIPD (les chiffres entre parenthèses se réfèrent aux critères du modèle d'analyse de seuil figurant à l'annexe 1 auxquels de telles opérations de traitement sont susceptibles de répondre):

- Bases de données d'exclusion (2, 4, 9);
- traitement à grande échelle de catégories particulières de données à caractère personnel (par exemple surveillance épidémiologique, pharmacovigilance, bases de données centrales aux fins de la coopération policière) (1, 4, 5, 8);
- analyse du trafic internet rompant le chiffrement (outils de prévention des pertes de données) (1, 3, 8);
- outils de recrutement électronique qui présélectionnent/excluent automatiquement des candidats sans intervention humaine (1, 2, 8).

Annexe 3

Liste non exhaustive d'opérations de traitement courantes ne nécessitant pas d'AIPD

Liste indicative d'opérations de traitement ne nécessitant à première vue pas d'AIPD lorsqu'elles sont effectuées par des institutions, organes et agences de l'Union agissant en tant que responsables du traitement uniques ou conjoints:

- Gestion de dossiers personnels au titre de l'article 26 du statut *en tant que telle*[33];
- procédures standard d'évaluation du personnel au titre du statut du personnel (évaluation annuelle);
- évaluations à 360° standard visant à aider des membres du personnel à élaborer des plans de formation;
- procédures standard de sélection du personnel;
- établissement des droits à la mise en service;
- gestion des congés, des horaires flexibles et du télétravail;
- systèmes de contrôle d'accès standard (non biométriques)[34];
- vidéosurveillance standard restreinte (pas de reconnaissance faciale, couverture limitée aux points d'entrée/sortie, uniquement sur le site, pas dans l'espace public).

[33] Certaines procédures entraînant l'ajout d'informations au fichier personnel peuvent nécessiter une AIPD, mais pas le dépôt de fichiers personnels en tant que tel.
[34] Par exemple, badges à présenter aux points d'entrée.

6 Documents de référence

Orientations relatives aux registres émanant des membres du comité

Certains membres du comité européen de la protection des données ont également publié des orientations et des explications sur la manière de consigner les opérations de traitement dans des registres en vertu des règles fonctionnellement équivalentes du RGPD:

- Commission belge de la protection de la vie privée: explications (FR/NL) et modèle de registre (FR/NL)
- Danemark: Datatilsynet: Vejledning om fortegnelse (janvier 2018)
- Allemagne (Datenschutzkonferenz): explications sur les registres et le modèle destiné aux responsables du traitement des données/sous-traitants
- Grèce: Autorité hellénique chargée de la protection des données Explications relatives aux registres et modèles destinés aux responsables du traitement des données/sous-traitants.
- Royaume-Uni: Information Commissioner's Office: explications et modèle

7 Glossaire

Le glossaire ci-dessous explique un certain nombre de termes relatifs à la protection des données utilisés dans la présente boîte à outils.

Adéquation (décision d')	La Commission peut décider qu'un pays tiers assure un niveau de protection adéquat des données à caractère personnel. Les transferts vers des pays tiers jugés adéquats ne nécessitent pas de garanties supplémentaires par rapport aux transferts vers des destinataires à l'intérieur de l'UE. Pour plus de détails, voir le chapitre V du règlement.
Analyse d'impact relative à la protection des données (AIPD)	Processus structuré de gestion des risques de protection des données associés à certaines opérations de traitement à risque (article 39 du règlement).
Analyse de seuil	Évaluation effectuée par le responsable du traitement, avec l'aide du DPD, pour déterminer si une AIPD est nécessaire.
Ancien règlement	Règlement (CE) 45/2001
Autorité chargée de la protection des données (APD)	Autorité publique chargée de superviser le traitement des données à caractère personnel. Le CEPD est l'APD des IUE.
Avis relatif à la protection des données	Avis d'information indiquant aux personnes concernées la manière dont un responsable du traitement traite leurs données à caractère personnel (articles 14 à 16 du règlement).
Catégories particulières de données	Données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, ou l'appartenance syndicale, et le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation

	sexuelle d'une personne physique (article 10 du règlement); données relatives aux condamnations pénales et aux infractions (article 11 du règlement).
Comité européen de la protection des données	Forum dans l'enceinte duquel les APD nationales, le CEPD et la Commission européenne coopèrent pour assurer une application cohérente des règles en matière de protection des données dans l'ensemble de l'UE. Il a remplacé le GT29.
Confidentialité	Caractéristique en vertu de laquelle des informations ne sont ni disponibles, ni divulguées à des personnes ou à des entités non autorisées, ni accessibles à des processus non autorisés.
Consentement	Toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement.
Contrôleur européen de la protection des données (CEPD)	Autorité de protection des données des IUE (voir le règlement).
Coordinateur de la protection des données (CPD)	Certaines grandes IUE ont des CPD qui font office de points de contact locaux dans chaque direction générale ou autre division organisationnelle analogue. Les CPD assistent le DPD.
Délégué à la protection des données (DPD)	Le DPD informe et conseille le responsable du traitement/l'IUE, le personnel de l'IUE et les personnes concernées sur les questions de protection des données et assure, de manière indépendante, l'application en interne des règles de protection des données au sein de leur IUE. Les DPD sont également la principale interface entre les IUE et le CEPD. Chaque IUE dispose d'un DPD.
Disponibilité	Caractéristique consistant à être accessible et utilisable à la demande par une entité autorisée.
Données à caractère personnel	Toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée «personne concernée»); est réputée être une «personne physique identifiable» une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale (article 4, paragraphe 1, du RGPD). Les personnes concernées peuvent être identifiables directement (par exemple, noms) ou indirectement (par exemple, «une directrice générale maltaise de votre IUE»).
Droit à l'effacement/droit à l'oubli	Les personnes concernées ont le droit d'obtenir l'effacement de leurs données à caractère personnel détenues par un responsable du traitement dans certaines situations, par exemple lorsque ces données sont détenues illégalement (article 19 du règlement).

Droit à l'information	Les personnes concernées ont le droit d'être informées du traitement que vous faites de leurs données à caractère personnel. Informez-les en fournissant un avis de protection des données/une déclaration de confidentialité.
Droit d'accès	Les personnes concernées ont le droit d'accéder à leurs données à caractère personnel détenues par un responsable du traitement; certaines dérogations peuvent s'appliquer (article 17 du règlement)
Droit de rectification	Les personnes concernées ont le droit d'obtenir la rectification de leurs données à caractère personnel détenues par un responsable du traitement lorsque celles-ci sont inexactes (article 18 du règlement).
Garanties adéquates	Mesures visant à assurer un niveau de protection adéquat lors du transfert de données à caractère personnel vers des pays tiers ou des organisations internationales, telles que des clauses contractuelles types
Gestion des risques	Processus de recensement, d'évaluation et de maîtrise/traitement des risques.
Gestion des risques de sécurité de l'information (GRSI)	Processus de gestion des risques visant à garantir que la confidentialité, l'intégrité et la disponibilité des actifs d'une organisation correspondent aux objectifs de celle-ci.
Institutions et organes européens (IUE)	Raccourci désignant l'ensemble des institutions, des organes, des bureaux, des agences et des autres entités européens qui entrent dans le champ d'application du règlement.
Intégrité	Caractère complet et exact des informations
(le) règlement	Règlement (UE) 2018/1725
Licéité du traitement	Pour être licite, le traitement des données à caractère personnel doit relever de l'une des situations énumérées à l'article 5 du règlement, comme être nécessaire à l'exécution d'une mission d'intérêt public dont est investie l'IUE au regard du droit européen.
Limitation du traitement	Marquage de données à caractère personnel conservées, en vue de limiter leur traitement à l'avenir (article 4, paragraphe 3, du RGPD).
Mesure de maîtrise	Dans la terminologie de la gestion des risques de sécurité de l'information, une mesure qui modifie le risque.
Notification de contrôle préalable	Notification au CEPD en vertu de l'article 27 du règlement (CE) nº 45/2001.
Notification de violation de données (à caractère personnel)	Notification obligatoire de violations de données (à caractère personnel) à l'autorité chargée de la protection des données.
Pays tiers	Pays non membres de l'UE ou de l'EEE; les transferts de données à caractère personnel vers des pays tiers peuvent nécessiter des garanties supplémentaires.
Personne compétente pour le compte du	Bien que votre IUE en tant que telle soit le responsable du traitement et reste comptable de ses opérations de traitement, la compétence est

responsable du traitement	généralement assumée à un niveau inférieur, par exemple par les propriétaires d'une opération de traitement spécifique.
Personne concernée	Toute personne physique dont vous traitez les données à caractère personnel, qu'elle soit ou non employée par votre IUE.
Profilage	Toute forme de traitement automatisé de données à caractère personnel consistant à utiliser ces données à caractère personnel pour évaluer certains aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des éléments concernant le rendement au travail, la situation économique, la santé, les préférences personnelles, les intérêts, la fiabilité, le comportement, la localisation ou les déplacements de cette personne physique (article 4, paragraphe 4, du RGPD)
Protection des données dès la conception et protection des données par défaut	Principe selon lequel les responsables du traitement doivent prendre en compte la protection des données à la fois pendant la conception et le déploiement de solutions et disposer de paramètres de protection par défaut (article 27 du règlement).
Qualité des données	Voir l'article 4 du règlement.
Registre	Documentation de vos opérations de traitement (article 31 du règlement).
Règlement général sur la protection des données (RGPD)	Règlement (UE) nº 2016/0679. Le RGPD établit les règles de protection des données applicables aux responsables du traitement du secteur privé et à la plupart des responsables du traitement du secteur public (à l'exception des missions de maintien de l'ordre) dans les États membres de l'UE.
Responsabilisation	Principe visant à assurer que les responsables du traitement soient de manière plus générale aux commandes et qu'ils soient en mesure de garantir et de démontrer le bon respect des principes en matière de protection des données dans la pratique. Le principe de responsabilité exige que les responsables du traitement mettent en place des mécanismes et systèmes de contrôle internes garantissant le respect des dispositions et fournissant des preuves de conformité (par exemple, des rapports d'audit) aux parties prenantes externes, y compris les organismes de surveillance.
Responsable du traitement	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; lorsque les finalités et les moyens dudit traitement sont déterminés par un acte spécifique de l'Union, le responsable du traitement ou les critères spécifiques applicables pour le désigner peuvent être prévus par le droit de l'Union [article 3, paragraphe 2, point b), du règlement].
Risque	Un événement possible qui pourrait causer des dommages ou pertes, ou affecter la capacité à atteindre les objectifs. Les risques ont une incidence et une probabilité. Peut aussi être défini comme l'effet de

	l'incertitude sur les objectifs.
Risque résiduel	Risque subsistant après le traitement du risque.
Sous-traitant	Personne physique ou morale, autorité publique, service ou tout autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement. Exemple: entreprise organisant un centre d'évaluation pour votre IUE, sur la base d'un contrat d'externalisation.
Traitement	Toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction (article 4, paragraphe 2, du RGPD).
Traitement des risques	Appliquer une mesure de maîtrise à un risque.
Violation de données (à caractère personnel)	Une atteinte à la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération ou la divulgation non autorisée de données à caractère personnel transmises, stockées ou traitées de quelque manière que ce soit, ou l'accès à ces données.