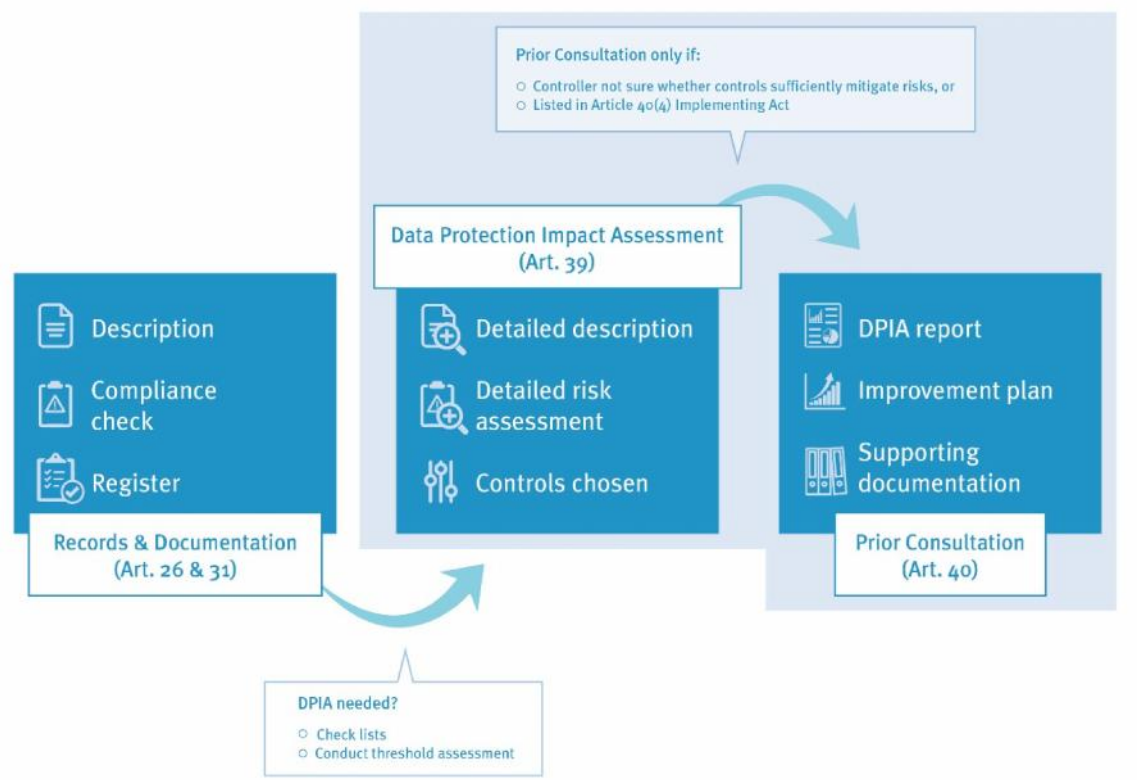
LE CONTRÔLEUR EUROPÉEN DE LA PROTECTION DES DONNÉES (CEPD)

Responsabilisation sur le terrain – Partie II: analyses d'impact relatives à la protection des données et consultation préalable

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
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 II: introduction et domaine d'application

Lorsque le traitement pose des «risques élevés», vous devez, en tant que personne compétente pour le compte du responsable du traitement, analyser et maîtriser les risques de manière plus approfondie, grâce à une analyse d'impact relative à la protection des données (AIPD). La partie II de la boîte à outils relative à la responsabilisation sur le terrain vous expliquera comment procéder. Dans certains cas, vous devrez peut-être également adresser une consultation préalable au CEPD. Cette procédure sera également abordée ici. Nous avons déjà vu, dans la partie I de la présente boîte à outils, comment générer des registres et documents connexes, et dans quels cas effectuer une AIPD.

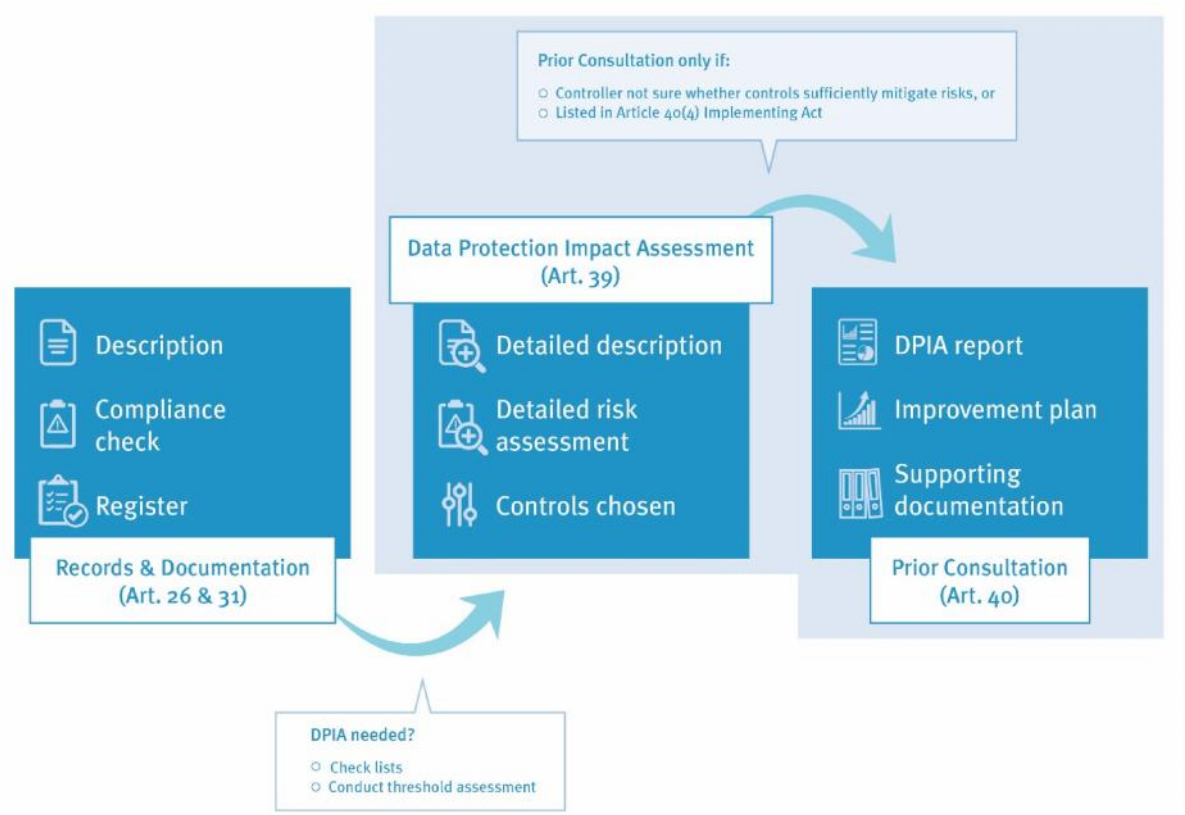


Figure 1: aperçu des obligations en matière de documentation

L'article 39, paragraphe 1, du règlement[1], prévoit qu'«[u]ne seule et même analyse peut porter sur un ensemble d'opérations de traitement similaires qui présentent des risques élevés similaires». Des **AIPD «conjointes» comme celles-là peuvent être indiquées lorsque plusieurs IUE effectuent des opérations de traitement de la même manière**, par exemple parce qu'elles possèdent des règles identiques pour des procédures spécifiques ou parce qu'elles utilisent le même produit de la même façon.

Si le rapport d'AIPD révèle qu'il subsiste des **risques résiduels élevés** (ou si le traitement figure dans une liste soumise à une obligation de consultation préalable), vous devrez consulter le CEPD en vertu de l'article 40 (voir la section 4 ci-dessous).

Le présent document couvre les aspects suivants:

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

- comment réaliser des AIPD,
- quand envoyer une AIPD au CEPD pour consultation préalable,
- qui fait quoi dans les processus ci-dessus,
- les règles de transition de l'ancien règlement 45/2001 applicables aux institutions de l'UE s'agissant des AIPD et de la consultation préalable.

Pour de plus amples informations sur la génération des registres et les critères permettant de décider s'il convient d'effectuer une AIPD, veuillez plutôt vous reporter à la partie I.

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].

Si vous êtes amené(e) à effectuer une AIPD, celle-ci relèvera également, conformément à l'article 39 du règlement, de la mission du responsable du traitement (dans la pratique: responsabilité de la direction, compétence du propriétaire du processus). Il prendra pour cela conseil auprès du DPD. Ce principe repose sur le raisonnement suivant: **puisque l'obligation redditionnelle incombe aux responsables du traitement, ceux-ci doivent également être propriétaires du processus d'AIPD**. Cela étant, les DPD sont souvent les personnes les plus qualifiées en matière de protection des données au sein des organisations, et ils peuvent jouer un rôle de guides et de facilitateurs dans le processus d'AIPD.

Le processus d'AIPD relève de la responsabilité et de la compétence des responsables du traitement, mais les DPD peuvent jouer un rôle important en les guidant tout au long du processus.

Pour les responsabilités/compétences des différents rôles dans votre organisation concernant les AIPD, voir ci-dessous:

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

[2] Article 3, paragraphes 1 à 8, du 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.

Service informatique			**X**	
Sous-traitants, le cas échéant			**X**	
Représentants des personnes concernées			**(X)**	

Figure 2: matrice RACI du processus d'AIPD

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, le service informatique fournira l'infrastructure technique et sera le mieux placé pour apporter son concours aux aspects de sécurité de l'information.

Le cas échéant, vous devrez également consulter les représentants des personnes concernées. Lorsque le traitement cible des membres du personnel des IUE, il s'agira souvent du comité du personnel. Si des personnes extérieures à votre IUE sont concernées, le responsable du traitement devra peut-être trouver des solutions pour également leur demander leur avis, le cas échéant. Cela **ne signifie pas nécessairement une consultation publique de toutes les parties intéressées.** Pensez, par exemple, à un système que votre IUE propose à des utilisateurs des administrations publiques des États membres, et dans lequel des données à caractère personnel de ces utilisateurs sont traitées. Dans ce cas, vous devrez peut-être consulter des représentants de la base d'utilisateurs, par exemple via le comité de pilotage du système ou des forums similaires. Lors de ces consultations, donnez aux représentants des personnes concernées un délai raisonnable pour réagir.

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. Comment effectuer une AIPD?

3.1 Exigences de base pour l'AIPD et choix de la méthode

Le processus d'AIPD vise à fournir l'assurance que les responsables du traitement (représentés ici par vous en tant que personne compétente au nom du responsable du traitement/propriétaire du processus) répondent de manière adéquate aux risques de confidentialité et de protection des données posés par les opérations de traitement «à risque». **En proposant une réflexion structurée sur les risques pour les personnes concernées et sur la manière de les atténuer, l'AIPD aide les organisations à se conformer à l'exigence de «protection des données dès la conception»** dans les cas où elle est le plus nécessaire, c'est-à-dire pour les opérations de traitement «à risque».

Bien que l'exécution de l'AIPD relève de votre compétence en tant que propriétaire du processus analysé, le DPD de votre IUE peut vous aider tout au long du processus – si vous avez besoin de conseils à n'importe quelle étape du processus, le DPD de votre IUE sera votre premier interlocuteur. Consultez également le DPD de votre IUE à chaque étape du processus d'AIPD.

Conformément à l'article 39, paragraphe 6, du règlement, une AIPD doit au minimum contenir les éléments suivants:

> *«a) une description systématique des opérations de traitement envisagées et des finalités du traitement;*
>
> *(b) une évaluation de la nécessité et de la proportionnalité des opérations de traitement au regard des finalités;*
>
> *(c) une évaluation des risques pour les droits et libertés des personnes concernées visés au paragraphe 1; et*
>
> *(d) les mesures envisagées pour faire face aux risques, y compris les garanties, mesures de sécurité et mécanismes visant à assurer la protection des données à caractère personnel et à apporter la preuve du respect du présent règlement, compte tenu des droits et des intérêts légitimes des personnes concernées et des autres personnes affectées.»*

Le **CEPD n'impose pas aux IUE de méthode standard pour la réalisation des AIPD**. Toutefois, **toute méthode utilisée doit être conforme aux exigences du règlement** et aux lignes directrices du GT29 concernant l'AIPD[4], qui proposent une interprétation des dispositions équivalentes du RGPD et ont été approuvées par le Comité européen de la protection des données. Les IUE sont libres d'utiliser toute méthode conforme. De nombreux membres du Comité européen de la protection des données possèdent déjà des méthodes d'AIPD ou sont en passe de s'en doter. Les organismes de normalisation et les associations industrielles peuvent également mettre des modèles au point.

Par souci de commodité, le **CEPD fournit à l'annexe 3 un exemple** pour les principes génériques des processus d'AIPD, dont un modèle de structure pour les rapports. Pour d'autres méthodes existantes, voir la première partie de l'annexe 4.

Le CEPD n'impose pas de méthode d'AIPD spécifique aux IUE. Vous pouvez avoir recours à toute méthode conforme aux règles, qu'il s'agisse de l'exemple fourni par le CEPD dans le présent document ou d'une autre méthode conforme aux lignes directrices du GT29/Comité européen de la protection des données.

Les AIPD sont **un processus cyclique** et non un exercice ponctuel. Si vous effectuez une AIPD lors de la conception d'un nouveau processus, celle-ci ne s'arrête pas une fois le processus adopté et déployé. Lorsque vous modifiez le processus, votre environnement de risque change. De même, après un certain temps, il est bon de réexaminer votre AIPD, de vérifier si elle reflète toujours la réalité et de la mettre à jour si nécessaire.

[4] WP248rev.01, https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236

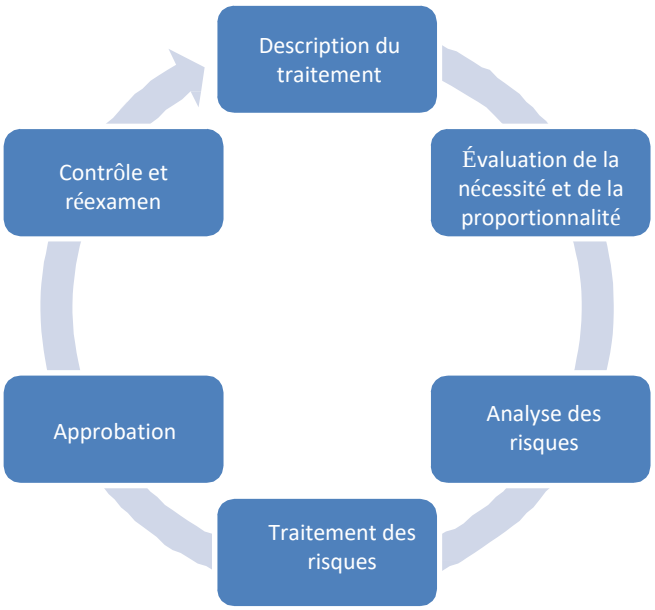


Figure 3: processus générique d'AIPD

Pour faire simple, vous commencez par une description de votre traitement – **«Que faisons-nous et comment?»** Il s'agira de la version longue des informations contenues dans le registre pour ce processus, avec un diagramme de flux de données. Expliquez également pourquoi vos organisations doivent effectuer cette opération de traitement et comment vous vous limitez à ce qui est nécessaire pour atteindre l'objectif du traitement (nécessité et proportionnalité) – **«Pourquoi le faisons-nous?»** Ensuite, vous évaluez les risques engendrés par le traitement. Il s'agit des risques pour les personnes concernées – **«Quelles seront les répercussions du traitement pour les personnes si tout se déroule comme prévu? Et si les choses se passent mal?»**, mais aussi les risques de conformité pour votre IUE – **«Sommes-nous autorisés à faire cela? Respectons-nous les obligations spécifiques que nous pourrions avoir?»** Ensuite, vous choisissez les mesures de maîtrise appropriées pour les risques identifiés – **«Que faisons-nous à ce sujet?»** Tout au long de ce parcours, vous documentez le processus et en faites rapport – **«... et notez bien tout»**. Lorsque vous arrivez à la fin de ce premier cycle (ou de tout cycle ultérieur) du processus, obtenez l'approbation de la direction concernée. Enfin, tenez à l'œil le fonctionnement des mesures de maîtrise retenues, l'évolution de votre environnement et/ou du processus – **«Est-ce que cela fonctionne? Cela reflète-t-il ce que nous faisons actuellement?»** – et mettez votre documentation à jour si nécessaire. L'annexe 3 fournit un modèle de structure pour les rapports d'AIPD comme ceux-là.

3.2 Description du traitement

Bien établir le contexte et décrire les opérations de traitement constitue le fondement d'un processus d'AIPD solide. En bref, vous devez décrire ce que vous prévoyez de faire et comment.

Cette documentation devrait permettre au lecteur de comprendre en quoi consiste le traitement et pourquoi vous le faites, qu'il s'agisse des personnes concernées par le traitement, de votre propre direction, qui devra approuver le rapport d'AIPD, du CEPD ou d'autres parties prenantes. Vous pouvez bien sûr vous référer à d'autres documents détenus par votre IUE, mais assurez-vous que la description est compréhensible en soi, car elle constituera un chapitre du rapport d'AIPD, lequel sera un document autonome.

La partie descriptive d'une AIPD commence par les informations contenues dans le registre, mais elle entre davantage dans les détails et comprend un diagramme de flux de données détaillé.

Pour créer cette description systématique du processus, commencez par les informations dont vous disposez déjà dans votre registre et ajoutez les points suivants:

- diagramme de flux de données (organigramme): quelles données recueillons-nous auprès de qui/où, qu'en faisons-nous, où les conservons-nous, à qui les communiquons-nous?
- description détaillée de la ou des finalités du traitement: expliquer le processus étape par étape, en faisant une distinction entre les finalités si nécessaire,
- description de ses interactions avec d'autres processus – ce processus repose-t-il sur des données à caractère personnel fournies par d'autres systèmes? Les données à caractère personnel de ce processus sont-elles réutilisées dans d'autres processus?
- description de l'infrastructure d'appui: fichiers, TIC, etc.

Vous voudrez peut-être utiliser la documentation existante du processus ou de sa conception pour générer cette documentation. Dans ce cas, relisez-la sous l'angle «comment cela affectera-t-il les personnes dont nous traitons les données?» et adaptez-la si nécessaire.

Une grande partie des informations requises pour l'AIPD existe probablement déjà dans votre IUE, dans la documentation de projet ou de processus conservée pour d'autres raisons, sans lien avec la protection des données. Vous voudrez peut-être réutiliser cette documentation dans la mesure du possible. Gardez toutefois à l'esprit que cette autre documentation est généralement rédigée en mettant l'accent sur votre IUE – «Que signifie ce processus pour notre IUE? Que doit faire notre IUE? Comment cela affecte-t-il notre IUE?» Dans le cadre de l'AIPD, l'accent est mis sur la façon dont le processus affecte les personnes dont les données sont traitées par votre IUE – si vous réutilisez la documentation existante aux fins de l'AIPD, passez-la en revue avec ce regard et soyez prêt(e) à l'adapter et à la développer si nécessaire.

3.3 Évaluation de la nécessité et de la proportionnalité

Conformément à l'article 39, paragraphe 6, point b), du règlement, vous devez également fournir une évaluation de la nécessité et de la proportionnalité du traitement. Dans cette section, expliquez pourquoi vous prévoyez d'effectuer le traitement. Veillez à expliquer que ce traitement est réellement nécessaire pour atteindre les objectifs de la base juridique; que le traitement répond efficacement à ce besoin et que le traitement est la solution la moins intrusive (du point de vue des droits fondamentaux) pour atteindre cet objectif (nécessité). Vous devez en outre veiller à ce que les avantages résultant du traitement ne soient pas inférieurs aux inconvénients qu'il engendre en matière de droits fondamentaux (proportionnalité).

Pour ce faire, expliquez:

a) en quoi les opérations de traitement proposées sont nécessaires pour permettre à votre organisation de remplir le mandat qui lui a été confié. Expliquez en quoi et pourquoi les opérations de traitement proposées sont un moyen efficace pour votre organisation de s'acquitter de sa mission et si vous avez envisagé d'autres solutions pour accomplir cette tâche, avec une indication de la raison pour laquelle l'approche retenue est la moins intrusive;

b) en quoi le traitement est proportionné à l'accomplissement de cette mission. Comparez les avantages du traitement avec les risques qu'il pose pour les droits fondamentaux. Il est possible qu'un traitement ayant passé avec succès le test de nécessité puisse néanmoins être considéré comme disproportionné.

3.4 Évaluation des risques

Une fois le contexte établi, votre prochaine étape consiste à analyser en détail les risques[5] engendrés par le traitement prévu. Il y a deux aspects à cela: les risques pour les droits et libertés des personnes concernées et ceux pour votre organisation. Ce ne sont pas nécessairement les mêmes.

L'AIPD vise prioritairement à évaluer les risques *pour les droits et libertés des personnes concernées*. Mais vous devez aussi, par la même occasion, analyser les *risques de conformité pour votre organisation*. Ces deux types de risques sont liés, mais pas identiques.

On entend par «risque», dans ce sens, un événement possible qui pourrait causer des dommages ou pertes, ou affecter la capacité à atteindre les objectifs. Les risques ont un *impact* («à quel point cela serait-il préjudiciable?») et une *probabilité* («quelle est la probabilité que cela se produise?»). Parmi les risques possibles en matière de protection des données figurent la divulgation non autorisée de données à caractère personnel ou de données inexactes conduisant à des décisions injustifiées concernant des personnes. Cette approche est bien connue de la gestion des risques de sécurité de l'information (GRSI) et de la planification de la continuité des activités, seuls les risques évalués sont différents. Ainsi, la planification de la continuité des activités s'attardera plutôt sur des risques tels que des coupures d'électricité, des inondations et des grèves des transports publics.

L'expression «droits et libertés» des personnes concernées se rapporte en premier lieu aux droits à la vie privée et à la protection des données (articles 7 et 8 de la charte), mais couvre également des droits connexes susceptibles d'être eux aussi affectés – pensez, par exemple, aux effets dissuasifs de mesures de surveillance sur la liberté d'expression ou la liberté de réunion. C'est l'évaluation visée à l'article 39, paragraphe 6, point c), du règlement.

Les risques pour votre organisation sont en fin de compte des risques de conformité – le non-respect des obligations de votre IUE concernant, par exemple, l'information de ceux dont vous traitez les données ou la nécessité d'assurer la sécurité des données en votre possession peut exposer votre IUE à des mesures réglementaires et lui donner mauvaise presse.

Dans certains cas, les risques peuvent varier: la divulgation illicite d'informations médicales porterait préjudice à la réputation de votre IUE, mais ne menacerait probablement pas son existence. En revanche, pour la personne dont les données ont été divulguées, les conséquences peuvent être plus graves.

[5] Les questions relatives à la détection des risques dans le modèle de registre annexé à la partie I renvoient à la première évaluation visant à déterminer si une AIPD peut être nécessaire. Ici, l'évaluation porte sur l'analyse des risques liés aux processus qui, selon vous, nécessitent une AIPD détaillée pour la conception des mesures de maîtrise requises.

Bien sûr, ces deux types de risques sont liés. Au fond, les obligations spécifiques auxquelles est soumise votre IUE sont des mesures de maîtrise déjà sélectionnées par le législateur de l'UE: il existe toujours un risque que des données soient réutilisées dans des contextes inattendus, d'où le principe de limitation de la finalité; le traitement des données sans information des personnes concernées empiète sur leur vie privée, d'où l'obligation pour les responsables du traitement d'informer les personnes dont ils traitent les données. En outre, les risques pour les personnes concernées finissent également par rejaillir sur votre organisation: ainsi, si l'adhésion à un nouvel outil est faible en raison de problèmes de confidentialité perçus, cela peut nuire aux ambitions de votre organisation pour cet outil; les violations de données et leurs coûts en matière d'image en sont un autre exemple évident.

Bien que tout cela comporte clairement un aspect de GRSI (notamment parce que la conservation sûre des données est l'un des principes de la protection des données), cet exercice est loin de s'y limiter. En effet, la gestion des risques de sécurité de l'information tend à se concentrer sur les risques qui découlent d'un comportement non autorisé du système (par exemple la divulgation non autorisée de données à caractère personnel), là où une partie des risques pour les personnes concernées et des risques de conformité sont engendrés par un comportement autorisé du système visé par l'AIPD.

Les processus qui fonctionnent exactement comme prévu peuvent avoir des répercussions sur les personnes concernées (par exemple, surveillance des employés). Ces risques doivent également être évalués, et pas seulement les risques que «les choses tournent mal». Pour ce faire, référez-vous aux principes de protection des données.

Ainsi, la capacité de surveiller la consommation d'électricité en temps réel à l'aide de compteurs intelligents, qui permet de tirer des conclusions sur le comportement des ménages (Qui est à la maison? Que font ces personnes?), est à la fois une caractéristique que les personnes concernées considèrent comme intrusive et une conséquence attendue de cette technologie. Pour prendre un exemple hypothétique dans une IUE, imaginez un système de gestion de dossiers intrusif qui suit toutes les actions et les renvoie en temps réel aux supérieurs hiérarchiques à des fins d'évaluation et de profilage du personnel (Combien de temps les personnes passent-elles sur chaque document? Quels sont leurs délais d'exécution par rapport à leurs collègues? Quel est leur rendement par rapport à leurs collègues? Qui pourrait/devrait être réaffecté à d'autres tâches?). Ce que le personnel trouverait probablement intrusif dans un tel système est précisément ce qu'il est censé faire.

Dans tous ces exemples, une approche GRSI classique ne tiendrait probablement pas compte de ces aspects. Bien qu'il existe un lien étroit avec la GRSI, puisque l'on ne peut avoir de bonne protection des données sans une bonne sécurité de l'information, les risques envisagés ici vont plus loin que les objectifs classiques de la GRSI, à savoir la confidentialité, l'intégrité et la disponibilité.

L'article 4 du règlement énumère les principes de protection des données[6]. D'autres articles y reviennent plus en détail:

[6] Voir l'annexe 2 de la Partie I pour de plus amples explications.

Principe de PD	Articles	Considérants
Loyauté	*Article 4, paragraphe 1, point a), et articles 17 à 25*	*20, 26, 34, 35, 37-41*
Transparence	*Article 4, paragraphe 1, point a), articles 14 à 16, article 25*	*20, 35, 36*
Limitation de la finalité	*Article 4, paragraphe 1, point b), articles 6 et 13*	*25*
Minimisation des données	*Article 4, paragraphe 1, point c), et articles 12, 13 et 36*	*20*
Exactitude	*Article 4, paragraphe 1, point d), article 18*	*38*
Limitation de la conservation	*Article 4, paragraphe 1, point e), article 13*	*20, 33*
Sécurité	*Article 4, paragraphe 1, point f), article 33*	*53*

Figure 4: principes de protection des données énoncés dans le règlement

Passez en revue votre diagramme de flux de données et, à chaque étape, demandez-vous comment cela pourrait affecter les personnes concernées à la lumière des principes de protection des données.

Partez des questions d'orientation ci-dessous pour réfléchir à ce qui pourrait affecter la réalisation de ces objectifs et à ce que pourrait en être l'impact sur les personnes concernées, en évaluant à la fois la gravité et la probabilité du risque. Il n'existe pas d'exigences spécifiques quant à l'échelle à utiliser pour cette évaluation, mais il peut être souhaitable d'utiliser des échelles que vos parties prenantes internes connaissent, par exemple parce que vous les utilisez dans votre processus de GRSI ou dans d'autres exercices de gestion des risques. La plupart des IUE utilisent une échelle à 5 points allant de «très faible» à «très élevé». Pour pouvoir disposer d'une évaluation cohérente des risques, définissez ce que signifie chaque niveau de l'échelle, par exemple du point de vue des répercussions sur la réputation ou les finances ou de la fréquence de la probabilité. Par exemple, divulguer des données médicales à des personnes sans besoin d'en connaître aura probablement plus de répercussions que la divulgation de coordonnées du personnel de l'IUE; de même, une divulgation à des agents de votre IUE ne disposant pas des autorisations nécessaires aura probablement un impact moindre qu'une divulgation accidentelle au grand public.

Pour cet exercice, parcourez votre diagramme de flux de données et demandez-vous à chaque étape comment celle-ci pourrait affecter ces objectifs. Certains objectifs sont plus pertinents que d'autres pour certaines étapes du traitement. Le tableau ci-dessous met en correspondance les objectifs avec certaines étapes génériques du traitement et mentionne les objectifs les plus pertinents pour chacune. Il s'agit des aspects à vérifier a minima.

	Loyauté	*Transparence*	*Limitation de la finalité*	*Minimisation des données*	*Exactitude*	*Limitation de la conservation*	*Sécurité*
Collecte	***X***	***X***	***X***	***X***	***X***		***X***
Fusion d'ensembles de données	***X***	***X***	***X***	***X***	***X***		***X***
Organisation/structuration			***X***	***X***	***X***		
Récupération/consultation/ utilisation	***X***	***X***	***X***		***X***	***X***	***X***
Édition/modification		***X***		***X***	***X***		***X***
Divulgation/transfert	***X***	***X***	***X***	***X***	***X***		***X***
Limitation			***X***	***X***	***X***	***X***	***X***
Stockage	***X***	***X***	***X***			***X***	***X***
Effacement/destruction			***X***			***X***	***X***

Figure 5: cartographie des éléments du diagramme de flux de données et des objectifs de protection

Pour cette évaluation des risques, passez en revue votre diagramme de flux de données et demandez-vous à chaque étape comment celle-ci pourrait affecter les objectifs de protection/principes de protection des données en vous aidant des questions d'orientation ci-dessous.

3.5 Questions d'orientation sur les principes de la protection des données

Partez des questions directrices ci-dessous à la fois pour analyser les différentes étapes et pour mener l'évaluation globale. Toutes les questions ne seront pas pertinentes pour toutes les étapes et, parfois, vous devrez davantage entrer dans les détails.

La **«loyauté»** du traitement comporte plusieurs aspects: le traitement est-il **inattendu** pour les personnes «touchées»? Cela a-t-il des **effets dissuasifs** sur l'exercice de leurs autres droits, rendant les personnes moins susceptibles de les exercer? Comment ces personnes peuvent-elles **intervenir** et faire entendre leur voix?

Le traitement est-il **inattendu** pour les personnes concernées, par exemple parce que vous réutilisez des données pour une finalité différente de celle pour laquelle elles ont été initialement collectées, ou parce que deux bases de données jusqu'alors séparées ont été fusionnées ou interconnectées à la suite d'une nouvelle législation? Même si les personnes concernées ne lisent pas l'avis de protection des données, pourraient-elles s'attendre à ce que cela se produise?

Dans le cas où vous vous fondez sur le consentement, assurez-vous que celui-ci est valable, libre et éclairé, faute de quoi votre traitement pourrait devenir illicite et déloyal (par exemple lorsque les gens consentent à une chose et que vous en faites une autre).

Troisièmement, demandez-vous si les opérations de traitement que vous prévoyez pourraient générer des **effets dissuasifs** pour l'exercice de leurs autres droits. Les «effets dissuasifs» réduisent la probabilité que des personnes exercent leurs droits fondamentaux. À titre d'exemple, pensez à une installation de vidéosurveillance dans une zone accessible au public située devant l'entrée de votre IUE et à la manière dont elle peut y affecter la liberté de réunion et d'expression.

Le troisième aspect de la loyauté, «garantir les droits des personnes à intervenir», renvoie collectivement aux droits d'accès, de rectification, d'effacement, de restriction du traitement, d'opposition et de portabilité des données dont jouissent les personnes en vertu du règlement. Elles doivent pouvoir recevoir une copie des données que vous détenez à leur sujet; les faire corriger si elles sont incorrectes; les faire effacer si vous les conservez de manière illicite; faire restreindre leur traitement dans certaines circonstances (par exemple en limitant leur visibilité à certains membres du personnel); s'opposer au traitement pour des motifs liés à leur situation particulière; et, dans certains cas, obtenir la portabilité des données.

Si les personnes ne sont pas en mesure, par exemple, de faire rectifier des informations incorrectes en temps utile, cela pourrait avoir des répercussions négatives sur elles. Vous devez vous assurer que les personnes concernées peuvent exercer ces droits au titre du règlement sans affecter les opérations de votre IUE.

Cela suppose, par exemple, de concevoir les systèmes de manière à pouvoir restreindre/verrouiller des entrées spécifiques d'une base de données sans entraver son fonctionnement ou de permettre aux personnes d'accéder facilement à leurs données à caractère personnel détenues dans un système en vue, notamment, de leur exportation. Vous devriez faciliter l'exercice des droits des personnes, par exemple en leur fournissant des informations faciles à trouver sur les points de contact et en portant d'emblée les exigences à leur connaissance (par exemple, comment elles peuvent prouver qu'elles sont bien la personne concernée lorsqu'elles demandent un accès). Pour plus d'informations sur tous ces droits, consultez les lignes directrices sur les droits des individus[7].

Questions d'orientation sur la loyauté

1. Les personnes peuvent-elles s'attendre à ce que cela se produise, même si elles ne lisent pas les informations que vous leur fournissez?
2. Si vous vous fondez sur le consentement, celui-ci a-t-il vraiment été donné librement? Comment documentez-vous que les personnes l'ont donné? Comment peuvent-elles révoquer leur consentement?
3. Cela pourrait-il générer des effets dissuasifs?
4. Cela pourrait-il déboucher sur une discrimination?
5. Est-il facile pour les personnes d'exercer leurs droits d'accès, de rectification, d'effacement, etc.?

Figure 6: questions d'orientation sur la loyauté

La **«transparence»** a été regroupée avec la loyauté à l'article 4, paragraphe 1, point a). Cela signifie que les personnes dont vous traitez les données doivent savoir que vous le faites et être en mesure de comprendre ce que vous faites de leurs données et pourquoi (articles 14 à 16 du règlement). Ce point est particulièrement important si vous ne collectez pas directement les données auprès des personnes concernées, mais auprès d'autres sources. Si vous avez une raison

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

licite de ne pas informer les personnes (ou de ne pas les informer d'emblée – pensez, par exemple, aux premières étapes d'une enquête de l'OLAF), vous devez réfléchir au moment où vous pourrez le faire et comment.

Si des personnes ne sont pas au courant que vous traitez leurs données à caractère personnel, elles ne peuvent pas exercer leurs autres droits au titre du règlement; en outre, si votre traitement repose sur le consentement, le fait de ne pas informer les personnes de manière appropriée signifie que leur consentement n'est pas valable. Pour plus d'informations, reportez-vous aux lignes directrices du CEPD sur les articles 14 à 16 du Règlement[8].

Questions d'orientation sur la transparence

1. Comment vous assurez-vous que les informations que vous fournissez parviennent effectivement aux personnes concernées?
2. Les informations que vous fournissez sont-elles complètes et faciles à comprendre?
3. S'adressent-elles au public visé? Les enfants, par exemple, peuvent avoir besoin d'informations adaptées.
4. Si vous reportez le moment d'informer les personnes, comment le justifiez-vous?

Figure 7: questions d'orientation sur la transparence

L'expression **«limitation de la finalité»** à l'article 4, paragraphe 1, point b), désigne le principe selon lequel les données à caractère personnel collectées dans un but ne doivent pas être réutilisées à d'autres fins incompatibles. Les IUE peuvent garantir ce principe à la fois au moyen de règles de conduite et par la conception des systèmes et des processus eux-mêmes. À cet égard, une caractéristique de conception importante peut souvent se révéler utile. Il s'agit de la «non-traçabilité». Ce concept fait référence à la propriété de ne pouvoir (facilement) relier des données à caractère personnel à d'autres informations concernant la même personne. Cela aide à faire respecter la limitation de la finalité et, par exemple, à empêcher la création de profils complets de personnes à des fins auxquelles celles-ci ne se seraient pas attendues.

L'archivage, la recherche scientifique, les fins historiques ou statistiques peuvent être considérés comme compatibles, mais nécessitent certaines garanties. Si vous souhaitez conserver/mettre à disposition des données à caractère personnel à de telles fins, réfléchissez à la manière dont cela pourrait affecter les personnes et dont vous pourriez réduire ce risque. Vous pourriez par exemple avoir recours à l'agrégation des données (dates de naissance transposées en tranches d'âge) ou différer la divulgation (ouverture des archives).

La limitation de la finalité agit comme un frein au détournement d'usage. Imaginez une situation dans laquelle des membres du personnel consulteraient un conseiller en orientation professionnelle de manière confidentielle, en précisant qu'ils aimeraient changer d'emploi, et que cette information soit réutilisée pour leur refuser une formation au motif qu'ils pourraient quitter l'organisation avant longtemps. Cela constituerait une infraction claire au principe de limitation de la finalité.

Questions d'orientation sur la limitation de la finalité

1. Avez-vous recensé toutes les finalités de votre processus?
2. Toutes les finalités sont-elles compatibles avec la finalité initiale?
3. Y a-t-il un risque que les données puissent être réutilisées à d'autres fins (détournement d'usage)?

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

4. Comment pouvez-vous vous assurer que les données ne seront utilisées qu'aux fins définies?
5. Si vous souhaitez mettre à disposition/ réutiliser des données à des fins de recherche scientifique, statistiques ou historiques, quelles garanties mettez-vous en place pour protéger les personnes concernées?

Figure 8: questions d'orientation sur la limitation de la finalité

La **«minimisation des données»** signifie que votre IUE ne traite que les données à caractère personnel dont elle a réellement besoin pour atteindre l'objectif du traitement et ne les conserve que le temps nécessaire à cet effet. Ce principe est également essentiel pour éviter le traitement excessif illicite de données à caractère personnel.

Cela suppose, par exemple, de vous assurer que vous ne demandez que les informations nécessaires dans vos formulaires et que vous ne conservez pas de données à caractère personnel «au cas où» vous pourriez en avoir l'usage plus tard. Les risques spécifiques ici pourraient être, par exemple, des paramètres par défaut dans des logiciels commerciaux standard qui entraîneraient le traitement de données à caractère personnel qui ne sont pas réellement nécessaires pour les finalités recherchées. Cela nécessite aussi de réfléchir à la question de savoir si les données que vous souhaitez collecter vous donnent réellement les informations que vous souhaitez obtenir. En d'autres termes, des données mesurent-elles ce que vous entendez mesurer?

Si vous prévoyez de mettre des données à caractère personnel à disposition à des fins archivistiques, à des fins de recherche scientifique ou historique ou à des fins statistiques sans rapport avec la finalité initiale du processus, réfléchissez à la manière dont cela pourrait affecter les personnes concernées et réduisez cet impact. Si vous pouvez remplir ces objectifs d'une manière qui n'implique pas de données à caractère personnel (par exemple, en conservant uniquement les données statistiques, mais pas les microdonnées), faites-le de cette manière. S'il est nécessaire de conserver des données à caractère personnel à ces fins, réfléchissez à la façon dont vous pouvez les minimiser (par exemple, en conservant des tranches d'âge au lieu de dates de naissance ou en agrégeant les données selon d'autres paramètres).

Questions d'orientation sur la minimisation des données

1. Les données que vous collectez mesurent-elles ce que vous entendez mesurer?
2. Pourriez-vous supprimer (ou masquer/cacher) certaines données sans compromettre l'objectif du processus?
3. Faites-vous clairement la distinction entre les données obligatoires et facultatives dans les formulaires?
4. Si vous souhaitez conserver des informations à des fins statistiques, comment gérez-vous le risque de réidentification?

Figure 9: questions d'orientation sur la minimisation des données

L'**«exactitude»** signifie que votre IUE est tenue de s'assurer que les informations qu'elle traite concernant les personnes sont exactes [article 4, paragraphe 1, point d), du règlement]. En effet, prendre des mesures sur la base d'informations inexactes peut avoir des répercussions négatives pour les personnes et engager la responsabilité de votre IUE. Si votre IUE s'aperçoit que des

informations sont inexactes ou incomplètes, elle est tenue de les rectifier[9] ou de les effacer sans délai. Permettre aux personnes concernées d'accéder facilement aux données peut être utile à cet égard. Dans certaines opérations de traitement, l'exactitude factuelle de déclarations peut être contestée par les parties concernées (par exemple les 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[10].

Questions d'orientation sur l'exactitude

1. La qualité des données est-elle suffisante pour l'objectif poursuivi?
2. Quelles pourraient être les conséquences pour les personnes concernées si des mesures ou des décisions étaient prises sur la base d'informations inexactes dans ce processus?
3. Comment vous assurez-vous que les informations que vous recueillez vous-même sont exactes?
4. Comment vous assurez-vous que les données que vous obtenez de tiers sont exactes?
5. Vos outils permettent-ils de mettre à jour/ corriger les données si nécessaire?
6. Vos outils permettent-ils d'effectuer des contrôles de cohérence[11]?

Figure 10: questions d'orientation sur l'exactitude

L'expression **«limitation de la conservation»** à l'article 4, paragraphe 1, point e), du règlement fait référence au fait que la conservation des données à caractère personnel doit être «aussi longue que nécessaire et aussi courte que possible». Dans certains cas, la législation de l'UE fixe des délais de conservation applicables à des opérations de traitement spécifiques, tandis que dans d'autres, il appartient à votre IUE de les définir. Déterminez vos délais de conservation en fonction de vos besoins pour le processus visé. Il ne s'agit pas d'une question technique, mais d'une question opérationnelle. La première question à se poser est celle du délai de conservation administrative, mais pensez également à ce que vous ferez au terme de celui-ci, en cas d'archivage.

Si vous souhaitez conserver les données (ou une partie de celles-ci) à des fins archivistiques, à des fins de recherche scientifique ou historique ou à des fins statistiques sans rapport avec la finalité initiale du traitement, réfléchissez à la manière dont cela pourrait affecter les personnes concernées (voir également «limitation de la finalité» ci-dessus). Veuillez noter que le 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

[9] Les modifications apportées en vue de rectifier des données à caractère personnel doivent pouvoir faire l'objet d'un audit sans affecter l'intégrité des données.

[10] 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 règlement.

[11] Par exemple, vérifier automatiquement si les dates de naissance saisies sont au bon format et se situent dans une plage plausible.

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.

Vous trouverez des indications sur les délais de conservation dans de nombreuses lignes directrices du CEPD relatives à des opérations de traitement spécifiques[12].

Questions d'orientation sur la limitation de la conservation

1. La législation de l'UE définit-elle des délais de conservation pour votre processus?
2. Combien de temps devez-vous conserver quelles données? À quelle(s) fin(s)?
3. Pouvez-vous établir des distinctions dans les délais de conservation de différents types de données?
4. Si vous ne pouvez pas encore supprimer les données, pouvez-vous en restreindre l'accès?
5. Vos outils permettront-ils un effacement permanent automatisé au terme du délai de conservation?

Figure 11: questions d'orientation sur la limitation de la conservation

Le terme **«sécurité»** à l'article 4, paragraphe 1, point f), renvoie aux notions de «confidentialité» et d'«intégrité», bien connues de la GRSI. On entend par «confidentialité» la caractéristique d'informations qui ne sont accessibles qu'aux personnes autorisées qui doivent en avoir connaissance. «Intégrité» désigne la caractéristique d'informations qui ne peuvent pas être modifiées sans autorisation adéquate[13]. Le troisième élément de la triade de la GRSI, la disponibilité, n'est pas inclus dans la liste figurant à l'article 4, paragraphe 1, point f), mais l'article 33, paragraphe 1, point c), souligne la nécessité de rétablir la «disponibilité» des données, et intègre ainsi également cette dimension essentielle de la sécurité de l'information.

Les violations de la confidentialité des données à caractère personnel peuvent causer divers types de préjudice, tels que la détresse psychologique (par exemple, fuite de données médicales) et un préjudice financier (par exemple, lorsque les données à caractère personnel divulguées sont utilisées pour un vol d'identité), aux individus. Pour éviter cela, vous devez concevoir vos systèmes de telle sorte que l'accès aux données à caractère personnel soit limité en vertu du strict principe du «besoin d'en connaître» et que les données à caractère personnel soient protégées contre la lecture par une personne non autorisée à tous les stades – que ce soit au repos ou en transit, au moyen d'un chiffrement le cas échéant. L'enregistrement des accès aux données à caractère personnel est un moyen de vous assurer de repérer toute violation possible et de pouvoir produire la preuve de qui a accédé aux données.

Les atteintes à l'intégrité des données à caractère personnel peuvent affecter les personnes si des décisions les concernant sont prises sur la base d'informations corrompues. Pour éviter cela, vous devez par exemple concevoir vos systèmes de telle sorte que les données à caractère personnel ne puissent être modifiées que par des utilisateurs autorisés et que ces modifications puissent faire l'objet d'un contrôle.

Les atteintes à la disponibilité empêchent l'utilisation même des données. Cela peut également affecter les personnes concernées (par exemple, impossibilité de payer les salaires si les données ne sont pas accessibles ou si le système est en panne) et l'exercice des droits des personnes concernées (accès, rectification, etc.).

[12] https://edps.europa.eu/data-protection/our-work/our-work-by-type/guidelines_en

[13] Si les informations peuvent être modifiées, ces changements doivent pouvoir faire l'objet d'un audit.

Pour cette cible, veuillez également vous reporter aux lignes directrices du CEPD sur les mesures de sécurité applicables au traitement des données à caractère personnel[14]. Votre organisation devrait également disposer d'une stratégie développée concernant la manière de gérer la sécurité de l'information en général, ce qui bénéficierait également à la protection des données.

Questions d'orientation sur la sécurité

1. Disposez-vous d'une procédure de recensement, d'analyse et d'évaluation des risques de sécurité de l'information pouvant affecter les données à caractère personnel et les systèmes informatiques qui sous-tendent leur traitement?
2. Ciblez-vous les répercussions sur les droits fondamentaux, les libertés et les intérêts des personnes et pas seulement sur les risques pour l'organisation?
3. Prenez-vous en considération la nature, la portée, le contexte et les finalités du traitement lorsque vous évaluez les risques?
4. Gérez-vous les vulnérabilités de votre système et les menaces pour vos données et vos systèmes?
5. Avez-vous des ressources et du personnel affectés à l'évaluation des risques?
6. Passez-vous systématiquement en revue et mettez-vous à jour les mesures de sécurité en fonction du contexte du traitement et des risques?

Figure 12: questions d'orientation sur la sécurité

Après avoir parcouru le diagramme de flux de données de cette façon, faites le point sur les risques recensés et demandez-vous si le traitement comporte des risques horizontaux qu'il n'est pas facile de lier à une étape spécifique. Assurez-vous de déceler ce type de risque également – parfois, le tout est plus que la somme de ses parties.

Ces questions ne sont qu'un point de départ, mais elles devraient vous aider à vous concentrer sur les aspects problématiques des opérations de traitement planifiées.

Une fois cette étape terminée, consignez vos résultats dans la documentation de l'AIPD. Plus le risque est élevé, plus vous devrez réfléchir à la conception des mesures de maîtrise à l'étape suivante.

3.6 Traitement des risques

Une fois les risques établis, vous devez choisir les mesures d'atténuation appropriées (maîtrise). La présente section décrit les approches possibles pour réduire les risques et propose quelques mesures de maîtrise génériques.

Veuillez noter que si le passage à une «approche fondée sur le risque» dans le RGPD et le règlement est une caractéristique majeure des nouvelles règles, il existe encore un certain nombre d'exigences spécifiques pour assurer la conformité et que votre organisation ne peut pas négliger celles-ci sans s'exposer à des actions réglementaires. Autrement dit, il y a des risques que votre organisation ne peut pas se contenter d'accepter, mais qu'elle doit atténuer ou prévenir. Considérez-les comme des mesures obligatoires prévues par le législateur parce qu'elles sont toujours judicieuses. Cela concerne notamment l'objectif de loyauté dans la protection. Votre IUE ne peut pas se borner à dire «nous ne fournirons pas d'accès, c'est trop

[14] https://edps.europa.eu/data-protection/our-work/publications/guidelines/security-measures-personal-data-processing_en et https://edps.europa.eu/data-protection/our-work/publications/guidelines/it-governance-and-it-management_en

compliqué», mais elle peut être en mesure de dire – le cas échéant – que «compte tenu du faible nombre de demandes auquel nous nous attendons dans ce nouveau système, nous n'investirons pas dans un système libre-service automatisé pour les personnes désireuses d'obtenir un accès, mais nous fournirons uniquement un point de contact et traiterons les demandes manuellement lorsqu'elles nous parviendront».

Lors de la sélection des mesures de maîtrise/d'atténuation, la conformité avec le règlement est la norme minimale sous laquelle vous ne pouvez pas descendre.

Les mesures de maîtrise peuvent cibler la probabilité (exemple: la sensibilisation du personnel des RH diminuera la probabilité qu'il divulgue des informations à des parties non autorisées, mais ne changera rien à l'impact si cela se produit), l'impact (exemple: s'assurer que les périphériques de stockage sont chiffrés réduit l'impact associé à l'oubli dans un train d'une clé USB contenant des données à caractère personnel, mais pas la probabilité que cela se produise), ou les deux. Dans certains cas, il se peut que vous soyez en mesure d'éviter complètement les risques (exemple: une refonte de processus supprime le besoin de données à caractère personnel – les données que vous ne détenez pas ne peuvent pas être divulguées de manière illicite).

Vous pouvez concevoir des mesures de maîtrise à partir de zéro, ou vous inspirer de catalogues de bonnes pratiques, tels que les orientations générales et spécifiques fournies par le CEPD[15] et d'autres APD; les lignes directrices d'organisations de normalisation nationales, européennes et internationales telles que le BSI, le CEN/CENELEC/ETSI et l'ISO; les lignes directrices d'organisations et de projets de sécurité de l'information tels que l'ENISA et l'OWASP; les orientations fournies par des travaux universitaires, des projets de recherche cofinancés par l'UE et des initiatives d'ingénierie de la sécurité et de la confidentialité telles que le réseau d'ingénierie de la vie privée sur l'internet[16], et les règles de sécurité de l'information de votre organisation. Assurez-vous que les mesures de maîtrise des risques choisies sont conformes au règlement.

À titre d'exemple, voici quelques mesures génériques regroupées suivant la façon dont elles contribuent à la maîtrise des risques:

- Prévention: prévenir la matérialisation des risques, par exemple:
  - sensibiliser le personnel afin de prévenir le partage de données non autorisé,
  - maintenir les délais de conservation et la quantité de données recueillies au minimum, afin qu'il y ait moins de données susceptibles d'être divulguées et que la tentation de modifier les finalités a posteriori soit réduite,
  - gérer les utilisateurs pour désactiver rapidement les droits d'accès des personnes qui n'ont plus besoin d'en connaître (par exemple parce qu'elles ont changé d'emploi);
  - séparer les données à caractère personnel de sorte que les violations de confidentialité dans un référentiel n'affectent pas les autres;
- Détection: surveiller vos opérations de traitement afin de vous assurer de repérer rapidement les violations, par exemple:

[15] Toujours à vérifier par rapport au contexte spécifique - les lignes directrices du CEPD donnent des recommandations générales; la manière dont elles peuvent être appliquées dans votre organisation peut dépendre des spécificités du processus.

[16] Pour plus d'informations et un référentiel d'informations, voir: https://ipen.trialog.com/wiki/Wiki_for_Privacy_Standards

- enregistrement des opérations et autosurveillance pour détecter les violations de données ou les utilisations illicites;
- garder une trace du moment et de la manière dont vous avez informé les personnes du traitement;

- Répression: veiller à avoir des mesures en place pour mettre fin rapidement aux violations détectées, par exemple:
  - procédures de rectification des données inexactes;
  - mécanismes de révocation des certificats pour mettre fin à l'utilisation d'identifiants compromis;
- Correction: veiller à avoir la possibilité de réparer ou de limiter les dommages après coup, par exemple:
  - conserver des sauvegardes, de manière à pouvoir revenir au statu quo ante après que les systèmes ont été compromis,
  - informer les destinataires après un transfert non autorisé et leur demander de supprimer les données.

Vous trouverez ci-dessous quelques exemples de mesures, regroupées par cible de protection. Comme les risques et donc les mesures à adopter dépendent des traitements spécifiques pour lesquels vous effectuez une AIPD, cette liste ne peut constituer qu'un point de départ.

Objectif	Mesures génériques
Loyauté	vérifier l'utilisation autorisée/prévue lors de la réutilisation d'ensembles de données
Transparence	notifier automatiquement les personnes concernées
Limitation de la finalité	restreindre les fonctionnalités d'exportation éviter les identifiants génériques
Minimisation des données	collecte de tranches d'âge plutôt que de dates de naissance
Exactitude	contrôles de cohérence contrôles de la qualité des données
Limitation de la conservation	établir une distinction dans les délais de conservation pour différentes parties des données, restreindre l'accès aux profils pertinents
Sécurité	se référer au cadre GRSI de votre IUE

Figure 13: liste indicative de mesures génériques par cible

Choisissez les mesures de maîtrise nécessaires pour assurer la conformité et atténuer les risques de manière appropriée.

Si vous estimez que des améliorations sont nécessaires pour atténuer les risques et les ramener à un niveau acceptable, créez un plan reprenant les améliorations que vous jugez nécessaires et un échéancier pour leur mise en œuvre.

3.7 Documentation et rapports

Le processus d'AIPD vous aide à réfléchir aux implications de vos opérations de traitement sur la vie privée et la protection des données. Afin de pouvoir prouver que vous avez suivi ce processus, vous devez le documenter.

Le principal produit livrable du processus d'AIPD est le rapport d'AIPD, qui résume les conclusions de cette section. Reportez-vous à l'annexe 3 pour un modèle de rapport d'AIPD.

Le rapport d'AIPD est le principal produit livrable du processus d'AIPD.

3.8 Cycles de réexamen

Les AIPD sont un processus, et non un exercice ponctuel. En ce sens, elles s'apparentent à d'autres processus de gestion comme la GRSI.

Choisissez la durée du cycle de réexamen en fonction des risques posés par vos opérations de traitement. Plus les risques sont élevés, plus le cycle de réexamen devrait être court. Le choix de la durée du cycle incombe au responsable du traitement. Par défaut, le CEPD recommande un cycle de réexamen de deux ans, avec un réexamen extraordinaire en cas de modifications significatives des opérations de traitement. D'autres circonstances peuvent nécessiter un réexamen extraordinaire, comme par exemple des violations de données importantes pointant que les contrôles de sécurité de votre IUE ne sont peut-être pas à la hauteur de la tâche. Des changements mineurs, tels que l'amélioration des contrôles de sécurité à la suite du processus d'amélioration continue de vos services, ne nécessitent pas nécessairement une mise à jour de l'AIPD: vérifiez si l'AIPD correspond toujours à votre traitement des risques et mettez-la à jour si nécessaire[17].

Il peut être intéressant de synchroniser ces cycles de réexamen avec d'autres examens réguliers des processus pertinents et de leur documentation (p. ex. GRSI ou mesures de contrôle internes).

Réexaminez régulièrement les rapports d'AIPD (suggestion: tous les deux ans) et préparez des réexamens extraordinaires au besoin.

3.9 Publicité des rapports d'AIPD

Le règlement n'exige pas expressément la publication des rapports d'AIPD. Cela dit, le CEPD considère la publication de ces rapports comme une bonne pratique. Vous devriez vous efforcer de publier au moins un résumé du rapport. Les parties des rapports qui ne devraient pas être divulguées au public, concernant par exemple les détails des mesures de sécurité, peuvent être supprimées le cas échéant[18].

Il peut être judicieux de documenter votre processus d'AIPD d'une manière qui permette de distinguer facilement les parties publiques (ou publiables) de la documentation de celles qui devraient rester internes. Le modèle de rapport d'AIPD de l'annexe 3 est structuré de manière à pouvoir choisir facilement les parties à publier et celles à usage interne.

[17] Exemple: l'un de vos contrôles organisationnels contre les atteintes à la confidentialité consiste à demander aux utilisateurs d'un système de signer des déclarations de confidentialité. Vous mettez à jour le texte de la déclaration pour le renforcer. Cela ne semble pas nécessiter une mise à jour du rapport d'AIPD.

[18] Veuillez noter qu'en tant que document détenu par votre IUE, la documentation complète de l'AIPD peut vous être demandée en vertu du règlement (CE) 1049/2001 sur l'accès du public.

Publier ces informations contribue également à rassurer vos parties prenantes et le grand public sur le fait que votre IUE respecte les règles relatives à la protection des données. Cela favorise la confiance et montre que les IUE donnent l'exemple en matière de respect des droits fondamentaux. Votre registre public et la partie du site web de votre IUE expliquant la politique soutenue par les opérations de traitement peuvent être de bons endroits où publier vos rapports d'AIPD.

«Faites de bonnes choses et parlez-en» – Publier vos rapports d'AIPD, au moins sous une forme résumée, est une bonne pratique. La publication permet de mettre en valeur le travail accompli pour rendre les opérations de traitement conformes et peut favoriser la confiance de vos parties prenantes et du grand public.

4. Quand procéder à une consultation préalable?

Seules certaines opérations de traitement nécessitant une AIPD requerront en outre une consultation préalable du CEPD. La consultation préalable concerne les cas «gris» où vous n'êtes pas certain(e) d'avoir atténué adéquatement les risques, mais qui ne sont pas tranchés au point que vous n'avez d'autre choix que d'abandonner le projet. Si vous vous trouvez dans une telle situation, consultez votre DPD.

L'article 40, paragraphe 1, du Règlement, précise qu'une consultation préalable est nécessaire lorsqu'une AIPD «indique qu'en l'absence de garanties, de mesures de sécurité et de mécanismes pour atténuer le risque, le traitement engendrerait un risque élevé pour les droits et libertés de personnes physiques et que le responsable du traitement est d'avis que ce risque ne peut être atténué par des moyens raisonnables, compte tenu des techniques disponibles et des coûts de mise en œuvre». Dans ce cas, le responsable du traitement – après consultation du DPD – doit consulter le CEPD[19]. Comme son nom l'indique, cette consultation doit avoir lieu avant le début des opérations de traitement.

Conformément aux lignes directrices du GT29 concernant les AIPD, toutes les opérations de traitement nécessitant des AIPD ne requièrent pas obligatoirement une consultation préalable.

1. Dans certains cas, la réalisation d'une AIPD et la mise en œuvre de mesures (supplémentaires) suffiront à atténuer les risques de manière appropriée et à les ramener à un niveau acceptable. Dans ce cas, une consultation préalable n'est pas nécessaire.
2. Dans d'autres cas, vous constaterez, à la suite de l'AIPD, que les risques ne peuvent pas être ramenés à un niveau acceptable. S'il se révèle impossible de mettre le projet en œuvre dans le respect des règles, vous devez l'abandonner.
3. Enfin, vous verrez parfois que des améliorations sont nécessaires pour atténuer les risques et les rendre acceptables et que les risques résiduels sont élevés. Ces cas «gris» sont ceux pour lesquels la consultation préalable est indiquée.

Sans préjudice de ce qui précède, la Commission européenne peut, conformément à l'article 4, paragraphe 4, du règlement, 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. La Commission

[19]L'article 39 du règlement (UE) 2016/794 impose à Europol une obligation spécifique de «consultation préalable» du CEPD. Il s'agit d'une obligation différente, avec des critères pertinents différents.

européenne ne l'a à ce jour pas fait. Si elle 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.

Voir ci-dessous pour un aperçu de la relation entre les «registres des activités de traitement» (article 31), les AIPD (article 39) et la consultation préalable (article 40). Toutes les opérations de traitement nécessitent des registres; certaines d'entre elles requièrent une AIPD; et certaines parmi ces dernières peuvent exiger une consultation préalable.

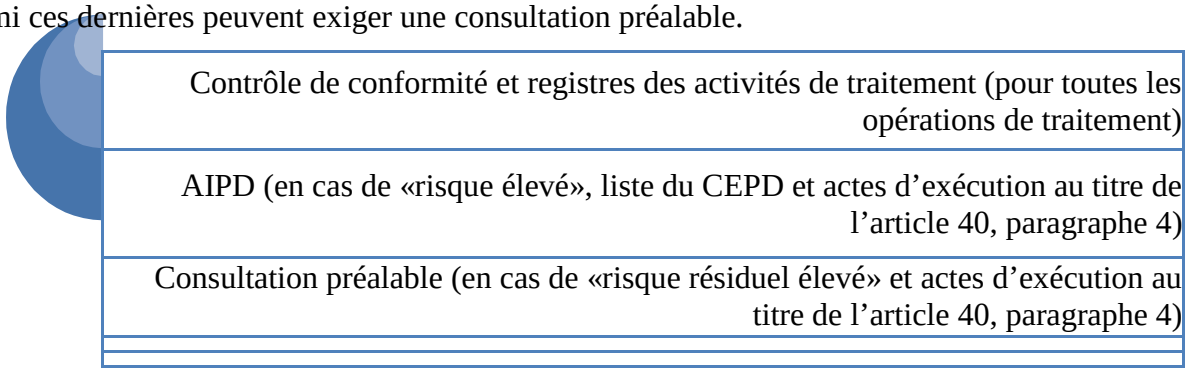


Figure 14: relation registres – AIPD – consultation préalable

Lorsque vous soumettez une consultation préalable, le CEPD analyse la documentation soumise et fournit des conseils sur les améliorations nécessaires. S'agissant du calendrier, vous devriez envoyer la consultation préalable à un stade où vous pouvez encore réagir aux recommandations contenues dans la réponse – si vous prévoyez de sous-traiter la conception du système appelé à sous-tendre les opérations de traitement prévues, alors le meilleur moment sera sans doute lorsque vous êtes en train de mettre la dernière main au cahier des charges/les clauses techniques de votre marché, avant de lancer l'appel d'offres.

La documentation à inclure dans la demande de consultation préalable sera essentiellement le rapport d'AIPD[20]. Veuillez fournir les documents suivants:

- le registre et le rapport complet de l'AIPD,
- le plan de traitement expliquant les améliorations des mesures de maîtrise prévues,
- la documentation connexe de votre processus GRSI,
- toute autre documentation que vous jugez nécessaire pour comprendre les risques posés par le traitement prévu et le choix des mesures.

Après réception d'une consultation préalable, le CEPD formulera des recommandations visant à assurer la conformité.

Conformément à l'article 40 du règlement, le délai imparti au CEPD pour formuler des recommandations est de huit semaines à compter de la réception de la consultation préalable, sans compter les suspensions pour les demandes d'informations complémentaires. Dans les cas complexes, ce délai peut être prolongé de six semaines supplémentaires dans un délai d'un mois à compter de la réception de la notification. Le CEPD informera les responsables du traitement (et les sous-traitants, le cas échéant) de cette prolongation et la motivera[21].

[20] Les éléments mentionnés à l'article 40, paragraphe 3, points a) à c), seront inclus dans le rapport d'AIPD de toute façon; et le point d) est en tout état de cause connu du CEPD.
[21] Pour les consultations préalables relevant du chapitre IX du règlement, les délais diffèrent: six semaines, avec une éventuelle prolongation de quatre semaines à communiquer dans le premier mois (article 90).

L'absence de réponse du Comité européen de la protection des données dans ce délai est sans préjudice d'éventuelles interventions ultérieures du CEPD (voir considérant 58 du règlement).

En vertu de l'article 27 de l'ancien règlement, vous deviez notifier certaines opérations de traitement «à risque» au CEPD pour contrôle préalable. Il existe toutefois des différences importantes entre ce contrôle préalable antérieur et les consultations préalables au titre du présent règlement:

- normes différentes pour le déclencher: risque résiduel au lieu du risque brut,
- l'absence de réponse ne vaut pas approbation.

Les critères différents signifient qu'il y aura moins de consultations préalables qu'il n'y avait de contrôles préalables.

5. Comment se préparer?

En tant que personne compétente pour le compte du responsable du traitement, vous n'aurez pas à créer votre documentation à partir de zéro. Les IUE effectuent déjà des opérations de traitement répondant aux critères d'exécution d'une AIPD. Nombre d'entre elles ont fait l'objet d'un contrôle préalable en vertu de l'article 27 de l'ancien règlement. Bien que les critères du contrôle préalable en vertu de l'ancien règlement et du nouveau règlement ne soient pas identiques, il existe un certain chevauchement – la plupart des opérations de traitement nécessitant une AIPD en vertu du règlement exigeaient déjà un contrôle préalable au titre de l'ancien règlement. D'autres opérations de traitement soumises à un contrôle préalable en vertu de l'ancien règlement ne nécessiteront pas d'AIPD.

Lors de vos préparatifs à l'application du nouveau règlement, examinez les cas soumis par le passé à un contrôle préalable. Certains d'entre eux pourraient également requérir une AIPD.

Veuillez vous reporter ci-dessous pour plus d'informations sur la façon de gérer les opérations de traitement existantes qui pourraient nécessiter une AIPD:

(i) Cas de contrôle préalable clos

Les opérations de traitement qui nécessiteront une AIPD et qui ont fait l'objet d'un contrôle antérieur avec un résultat positif (avec une procédure de suivi close, le cas échéant) en vertu de l'ancien règlement peuvent bénéficier d'un délai de grâce de deux ans, de sorte qu'aucune AIPD n'est requise dans l'immédiat.

Toutefois, si/lorsque les procédures et/ou les risques changent, une AIPD sera nécessaire afin de vérifier la conformité avec le règlement.

(ii) Avis de contrôle préalable toujours en phase de suivi:

Si le suivi des opérations de traitement qui nécessitaient un contrôle préalable en vertu de l'article 27 de l'ancien règlement et une AIPD en vertu du règlement n'était pas terminé lorsque le règlement est devenu applicable, vous devez vérifier si une AIPD est requise en procédant à une analyse de seuil (voir partie I - section 4). Si celle-ci confirme la nécessité d'une AIPD, commencez-la immédiatement.

6. Conclusion

La partie II de la *boîte à outils sur la responsabilisation* vous a fourni des conseils pratiques sur la manière de réaliser les AIPD et sur les situations où vous devez en outre consulter le CEPD au préalable.

En tant que propriétaire du processus, c'est vous qui êtes aux commandes – la conformité avec 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 AIPD sont un outil important pour gérer les risques de confidentialité et de protection des données pour vos opérations de traitement «plus à risque». Le fait d'avoir passé le processus en revue prouve que vous avez pensé à ces risques et avez choisi des moyens justifiables de les gérer. 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 AIPD. La non-exécution des AIPD nécessaires peut valoir une amende administrative à votre IUE[22].

Pour les cas particulièrement difficiles, procédez à une consultation préalable du CEPD; dans sa réponse, le CEPD vous fournira des conseils supplémentaires sur la manière d'assurer le respect des règles de protection des données. Conformément à l'esprit de «responsabilisation» du règlement, nous ne nous attendons pas à ce qu'il y ait beaucoup de consultations préalables. Et à tout le moins, nous nous attendons à ce qu'il y en ait moins que de notifications de contrôle préalables au titre de l'ancien règlement.

[22] Article 66 du règlement. Un projet de document d'orientation a été envoyé aux DPD pour information.

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:

- rédiger des projets d'AIPD,
- analyser s'il convient de procéder à une consultation préalable.

DPD:

- guider les responsables du traitement tout au long du processus d'AIPD;
- fournir des commentaires sur l'ébauche de la documentation/les AIPD;
- répondre aux consultations des responsables du traitement/propriétaires de processus,
- assurer l'interface entre l'IUE et le CEPD, notamment en soumettant des consultations préalables.

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. Catalogue des questions d'orientation par principe de protection des données

Questions d'orientation sur la loyauté

1. Les personnes peuvent-elles s'attendre à ce que cela se produise, même si elles ne lisent pas les informations que vous leur fournissez?
2. Si vous vous fondez sur le consentement, celui-ci a-t-il vraiment été donné librement? Comment documentez-vous le fait que les personnes l'ont donné? Comment peuvent-elles révoquer leur consentement?
3. Cela pourrait-il générer des effets dissuasifs?
4. Cela pourrait-il déboucher sur une discrimination?
5. Est-il facile pour les personnes d'exercer leurs droits d'accès, de rectification, d'effacement, etc.?

Questions d'orientation sur la transparence

1. Comment vous assurez-vous que les informations que vous fournissez parviennent effectivement aux personnes concernées?
2. Les informations que vous fournissez sont-elles complètes et faciles à comprendre?
3. S'adressent-elles au public visé? Les enfants, par exemple, peuvent avoir besoin d'informations adaptées.
4. Si vous reportez le moment d'informer les personnes, comment le justifiez-vous?

Questions d'orientation sur la limitation de la finalité

1. Avez-vous recensé toutes les finalités de votre processus?
2. Toutes les finalités sont-elles compatibles avec la finalité initiale?

3. Y a-t-il un risque que les données puissent être réutilisées à d'autres fins (détournement d'usage)?
4. Comment pouvez-vous vous assurer que les données ne seront utilisées qu'aux fins définies?
5. Si vous souhaitez mettre à disposition/ réutiliser des données à des fins de recherche scientifique, statistiques ou historiques, quelles garanties mettez-vous en place pour protéger les personnes concernées?

Questions d'orientation sur la minimisation des données

1. La qualité des données est-elle suffisante pour l'objectif poursuivi?
2. Les données que vous collectez mesurent-elles ce que vous entendez mesurer?
3. Pourriez-vous supprimer (ou masquer/cacher) certaines données sans compromettre l'objectif du processus?
4. Faites-vous clairement la distinction entre les données obligatoires et facultatives dans les formulaires?
5. Si vous souhaitez conserver des informations à des fins statistiques, comment gérez-vous le risque de réidentification?

Questions d'orientation sur l'exactitude

1. Quelles pourraient être les conséquences pour les personnes concernées si des mesures ou des décisions étaient prises sur la base d'informations inexactes dans ce processus?
2. Comment vous assurez-vous que les informations que vous recueillez vous-même sont exactes?
3. Comment vous assurez-vous que les données que vous obtenez de tiers sont exactes?
4. Vos outils permettent-ils de mettre à jour/ corriger les données si nécessaire?
5. Vos outils permettent-ils d'effectuer des contrôles de cohérence?

Questions d'orientation sur la limitation de la conservation

1. La législation de l'UE définit-elle des délais de conservation pour votre processus?
2. Combien de temps devez-vous conserver quelles données? À quelle(s) fin(s)?
3. Pouvez-vous établir des distinctions dans les délais de conservation de différents types de données?
4. Si vous ne pouvez pas encore supprimer les données, pouvez-vous en restreindre l'accès?
5. Vos outils permettront-ils un effacement permanent automatisé au terme du délai de conservation?

Questions d'orientation sur la sécurité

1. Disposez-vous d'une procédure de recensement, d'analyse et d'évaluation des risques de sécurité de l'information pouvant affecter les données à caractère personnel et les systèmes informatiques qui sous-tendent leur traitement?
2. Ciblez-vous les répercussions sur les droits fondamentaux, les libertés et les intérêts des personnes et pas seulement sur les risques pour l'organisation?
3. Prenez-vous en considération la nature, la portée, le contexte et les finalités du traitement lorsque vous évaluez les risques?
4. Gérez-vous les vulnérabilités de votre système et les menaces pour vos données et vos systèmes?
5. Avez-vous des ressources et du personnel affectés à l'évaluation des risques?

6. Passez-vous systématiquement en revue et mettez-vous à jour les mesures de sécurité en fonction du contexte du traitement et des risques?

3. Modèle de structure pour le rapport de l'AIPD

La structure ci-dessous peut servir de modèle au rapport d'une AIPD.

1. **Nom du projet**
2. **Validation/approbation**

   Chaîne d'approbation et approbation
3. **Réexamen**

   Fournissez des informations sur le cycle de réexamen, l'état actuel et des informations de versionnement pour les itérations précédentes
4. **Synthèse**

   Donnez un bref aperçu des principales conclusions de l'AIPD: principaux risques recensés, mesures retenues…
5. **Motif de cette AIPD**

   Expliquez rapidement: a) figurant sur la liste positive ou b) résultat d'une analyse de seuil
6. **Principaux acteurs**

   Fournissez une vue d'ensemble de qui a été associé quand et sur quels aspects
7. **Description du traitement**

   Sur la base des informations contenues dans le registre de l'opération de traitement, préparez ce qui suit:

   - *diagramme de flux de données (organigramme): quelles données recueillons-nous auprès de qui/où, qu'en faisons-nous, où les conservons-nous, à qui les communiquons-nous?*
   - *description détaillée de la ou des finalités du traitement: expliquer le processus étape par étape, en faisant une distinction entre les finalités si nécessaire,*
   - *description de ses interactions avec d'autres processus – ce processus repose-t-il sur des données à caractère personnel fournies par d'autres systèmes? Les données à caractère personnel de ce processus sont-elles réutilisées dans d'autres processus?*
   - *description de l'infrastructure d'appui: fichiers, TIC, etc.*
8. **Nécessité et proportionnalité**

   Sur la base des informations contenues dans le registre de l'opération de traitement, expliquez ce qui suit:

   - *en quoi les opérations de traitement proposées sont nécessaires pour permettre à votre IUE de remplir le mandat qui lui a été confié?*
   - *en quoi le traitement reste-t-il proportionné à l'accomplissement de cette mission?*
9. **Analyse des risques et mise en place de mesures de maîtrise des risques identifiés**

   Vous pouvez vous baser sur la liste de l'annexe 2.

N°	Élément dans l'organigramme des données	Description du risque	Principe(s) de protection des données associé(s)	Gravité (brute)	Probabilité (brute)	Mesures de maîtrise	Gravité (résiduelle)	Probabilité (résiduelle)
1	Dépôt électronique de dossiers personnels	Usage secondaire non autorisé	Limitation de la finalité, sécurité	3	3	Le personnel reçoit une formation à la PD La liste de contrôle d'accès limite l'accès à ceux qui ont besoin d'en connaître. Les accès sont consignés et les journaux analysés; voir les points A, B, C de	3	1
2	Dépôt électronique de dossiers personnels	Corruption de données	Qualité des données, sécurité	4	1	Les modifications sont consignées et les sauvegardes conservées	1	1
…								
n								

10. Commentaires de la PC

Qui avez-vous consulté? Quels ont été leurs commentaires et préoccupations? Comment les avez-vous intégrés (par exemple en ajoutant des risques supplémentaires à la section 7 ci-dessus)?

11. Commentaires du DPD

Quels ont été les commentaires et préoccupations du DPD? Comment les avez-vous intégrés (par exemple en ajoutant des risques supplémentaires à la section 5 ci-dessus)?

4. Documents de référence

4.1.Autres méthodes d'AIPD émanant des membres du Comité européen de la protection des données

Si vous ne souhaitez pas utiliser la méthode proposée dans le présent document, vous êtes libre d'utiliser l'une des méthodes ci-dessous, à condition qu'elle ait été mise à jour si nécessaire pour être conforme au RGPD /au règlement:

- Commission belge de la protection de la vie privée: LD AIPD (FR/NL)
- DanemarkDatatilsynet – Konsekvensanalyse (mars 2018)
- Allemagne (Datenschutzkonferenz): Modèle standard de protection des données, V.1.0 – Version d'essai, unanimement et affirmativement reconnue (avec abstention de la Bavière) par la 92e Conférence des autorités indépendantes de protection des données de l'État fédéral et des Länder, qui s'est tenue à Kühlungsborn les 9 et 10 novembre 2016: DE / EN
- Agence espagnole de protection des données – Guía práctica de Evaluaciones de impacto (2018)
- CNIL (France)
  - Outil logiciel PIA (mis à jour en 2018)
  - CNIL, Guides AIPD 1 (La méthode), 2 (Les modèles et les bases de connaissances) et 3 (Les bonnes pratiques)de juillet 2015
- APD slovène: Smernice ocene učinkov na varstvo osebnih podatkov (2018)
- UK Information Commissioner Data Protection Impact Assessments (mai 2018)

4.2.Autres méthodes d'AIP(D) émanant de tiers

Les présentes méthodes ont été adoptées par d'autres tiers, tels que des autorités chargées de la protection des données dans les pays tiers. Elles peuvent ne pas être conformes aux normes énoncées dans le RGPD ou le règlement et sont incluses à titre d'information uniquement:

- Australian Information Commissioner - Guide to undertaking privacy impact assessment (mai 2014)
- Commissariat à la protection de la vie privée du Canada – Guide au sujet du processus d'évaluation des facteurs relatifs à la vie privée (mars 2011)
- New Zealand's Privacy Commissioner (2015) – Privacy Impact Assessment Toolkit
- USA DHS – PIA guidance & template (juin 2010)
- USA SEC – PIA guide (janvier 2007)
- USA NIST – An Introduction to Privacy Engineering and Risk Management in Federal Systems (janvier 2017)
- Ireland HIQA – Guidance on Privacy Impact Assessment in Health and Social Care (décembre 2010)ISO/IEC 29134:2017
- ISACA GDPR Data Protection Impact Assessments (2017)
- NL NOREA – De beroepsorganisatie van IT-auditors (novembre 2015)
- Forum Privatheit: White Paper Datenschutz-Folgenabschätzung - Ein Werkzeug für einen besseren Datenschutz, dritte, überarbeitete Auflage, partiellement basé sur le modèle standard de protection des données

4.3.Rapports de recherche et littérature universitaire

- Bieker F., Friedewald M., Hansen M., Obersteller H., Rost M. (2016): A Process for Data Protection Impact Assessment under the European General Data Protection Regulation, in: K. Rannenberg, D. Ikonomou (eds.): Privacy Technologies and Policy. Fourth Annual Privacy Forum, APF 2016 Frankfurt. Heidelberg, New York, Dordrecht, London
- Bieker F., Hansen M., Friedewald M. (2016): Die grundrechtskonforme Ausgestaltung der Datenschutz-Folgenabschätzung nach der neuen europäischen Datenschutz-Grundverordnung, RDV 2016, issue 4, p. 188
- Hansen M. (2016): Datenschutz-Folgenabschätzung – gerüstet für Datenschutzvorsorge?, DuD 9/2016, S. 587
- Ireland HIQA (2010): International Review of Privacy Impact Assessments
- PIAF project consortium (de Hert, Paul et al.) deliverables: Review and analysis of existing PIA (2011), survey of DPAs on PIAs (2012), Final report with recommendations for a EU PIA framework (2012), project homepage
- Wright D., Finn R., Rodrigues R. (2013): A Comparative Analysis of Privacy Impact Assessment in Six Countries, Journal of Contemporary European Research (JCER), 9 (1), p. 160

5. 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	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	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

l'oubli	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	Notification obligatoire de violations de données (à caractère personnel) à l'autorité chargée de la protection des données.

personnel)	
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 responsable du traitement	Bien que votre IUE en tant que telle soit le responsable du traitement et reste comptable de ses opérations de traitement, la compétence est 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. Ce principe 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.