Analyse d'impact relative à la protection des données dans l'Union européenne : élaboration d'un modèle de rapport du processus d'analyse

Dariusz Kloza, Alessandra Calvi, Simone Casiraghi, Sergi Vazquez Maymir, Nikolaos Ioannidis, Alessia Tanas, Niels van Dijk

Analyse d'impact relative à la protection des données dans l'Union européenne : élaboration d'un modèle de rapport du processus d'analyse

d.pia.lab Note de Politique N° 1/2020

Dariusz KLOZA, Alessandra CALVI, Simone CASIRAGHI,
Sergi VAZQUEZ MAYMIR, Nikolaos IOANNIDIS, Alessia TANAS et Niels VAN DIJK

Laboratoire bruxellois de l'analyse d'impact relative à la protection des données et de la vie privée (d.pia.lab)
Research Group on Law, Science, Technology & Society (LSTS) | Vrije Universiteit Brussel (VUB)

La présente Note de Politique propose un modèle de rapport du processus d'analyse d'impact relative à la protection des données (AIPD) dans l'Union européenne (UE). Basé sur le cadre et la méthode pour l'analyse d'impact précédemment élaborés (voir respectivement la Note de Politique N° 1/2017 et la Note de Politique N° 1/2019), le modèle proposé est conforme aux exigences des Articles 35–36 du Règlement Général sur la Protection des Données (RGPD) et reflète les meilleures pratiques relatives à l'analyse d'impact. Il présente en outre cinq nouveaux aspects. Premièrement, il vise l'exhaustivité afin de fournir les conseils les plus avisés et robustes possibles pour la prise de décision. Deuxièmement, il vise l'efficacité, dans le sens où il veut produire des effets tout en utilisant le moins de ressources possible. Troisièmement, il vise à examiner et accommoder les points de vue des différentes parties prenantes, même si le point de vue des particuliers sera prédominant. Pour cette raison, il favorise la réflexion sur les droits fondamentaux, notamment en exigeant une justification pour chaque choix à réaliser, ce qui va au-delà d'une simple opération consistant à « cocher une case ». Quatrièmement, il vise à adopter l'approche de « legal design » afin de guider les évaluateurs d'une manière pratique, aisée et intuitive à travers les 11 étapes du processus d'analyse en fournissant les explications nécessaires à chaque étape, tout en offrant une structure composée de champs à compléter et de tableaux extensibles et modifiables. Cinquièmement, il accepte de ne pas être définitif du fait qu'il devra être révisé au fur et à mesure de l'expérience acquise lors de son utilisation. Le modèle est principalement destiné aux évaluateurs auxquels les responsables du traitement de données ont confié la réalisation du processus d'analyse, mais il peut également aider les autorités de protection des données (APD) au sein de l'UE à développer (adapter) des modèles pour les AIPD se rapportant au champ de leurs propres compétences.

1 INTRODUCTION

1.1 CONTEXTE

Le Règlement Général sur la Protection des Données (RGPD) de l'Union européenne (UE) impose aux responsables du traitement de données, *inter alia*, de conduire un processus d'analyse d'impact relative à la protection des données (AIPD) (Article 35(1)), notamment lorsqu'il y a une probabilité de risque élevé pour les droits et libertés des personnes physiques. Cette nouvelle exigence a déjà suscité toute une série de questions, dont certaines concernent les aspects pratiques du processus d'analyse. En réponse, d.pia.lab propose dans la présente Note de Politique un *modèle* de rapport pour un processus AIPD lequel reflète les meilleures pratiques pour l'analyse d'impact tout en étant conforme aux exigences du RGPD.

Un tel modèle constitue un outil pratique qui aidera les évaluateurs lors du processus d'analyse. Il consiste d'un formulaire à compléter qui structure le processus d'analyse suivant une méthode déterminée et guide les évaluateurs à travers celui-ci. Une fois finalisé, il sert de base au rapport final. Parallèlement, le rapport documente toutes les activités entreprises au sein d'un processus d'analyse déterminé, et permet aux responsables du traitement de données, *inter alia*, de démontrer la mesure dans laquelle leur manière de traitement de données est conforme à la loi, tout en fournissant des éléments de preuve par rapport à la qualité du processus d'analyse (voir aussi le principe de la responsabilité ; Article 5(2)). Un modèle de processus d'analyse peut être considéré comme la mise en œuvre pratique d'une *méthode* d'analyse d'impact (c.-à-d. une procédure constituée d'étapes consécutives et/ou itératives), lequel offre à son tour un *cadre* (c.-à-d. des conditions

 ISSN 2565-9936

et des principes définissant sa théorie et sa mise en pratique). En dépit de leurs avantages, les modèles de processus de l'analyse d'impact présentent leurs propres limites qui sont inhérentes à ce type d'instrument. Ils ne peuvent donc être utilisées sans réflexion critique.

1.2 PROGRÈS TECHNIQUES ET AU-DELÀ

Il n'existe aucun consensus sur la façon *exacte* dont il faut exécuter un processus d'analyse d'impact. Plusieurs modèles ont été développés pour le processus AIPD, prenant différentes formes et présentant différentes possibilités d'application (domaines de compétence, secteur industriel, secteur de gouvernance, etc.) La qualité de ces modèles varie considérablement. Les problèmes les plus fréquemment observés semblent concerner leur inadéquation à l'objectif poursuivi et leur manque d'exhaustivité, de clarté et de détails, ce qui les rend peu utiles aux évaluateurs.

Le modèle proposé est basé sur une analyse critique et comparative des modèles existants, améliorés en fonction de l'expérience acquise par d.pia.lab. Le modèle souscrit aux principes et conditions définis dans le *cadre* pour l'analyse d'impact développé par d.pia.lab (voir la Note de Politique N° 1/2017, Sect. 2). Il est basé sur la *méthode* générique pour la réalisation d'une analyse d'impact (voir la Note de Politique N° 1/2019, Sect. 2), légèrement révisée et mise à jour, et adaptée aux exigences légales qui sont d'application au sein de l'UE (voir la Note de Politique N° 1/2019, Sect. 3). Autrement dit, le modèle combine la méthode générique avec la méthode spécifique pour un processus AIPD, tel qu'il est interprété à partir des Articles 35–36, principalement en superposant le dernier au premier. Le modèle fait cependant la différence entre les éléments obligatoires et facultatifs du processus d'analyse. Il en résulte que tout élément qui n'est pas *expressément formulé* comme étant obligatoire par le RGPD, est clairement indiqué comme tel.

Le modèle proposé présente au moins cinq nouveaux aspects. Premièrement, il veut être exhaustif et apporter les conseils les plus avertis et solides possibles pour la prise de décision. A cet effet, il vise à inclure les préoccupations sociétales pertinentes, les parties prenantes et les étapes à suivre au cours du processus d'analyse, pour ne citer que ces aspects-là.

Deuxièmement, le modèle vise à rendre le processus AIPD plus efficace, c.-à-d. qu'il veut produire des effets (p.ex. fournir des conseils pour faciliter la prise de décision) tout en utilisant le moins de ressources possible. Ainsi, il permet la sélection de certaines techniques d'évaluation particulières ou l'intégration de plusieurs processus d'analyse. En vue d'optimiser l'utilisation des ressources, le modèle prévoit une étape spécifique afin de planifier et préparer un processus d'analyse déterminé.

Troisièmement, le modèle vise à examiner et accommoder les points de vue de différentes parties prenantes, telles que les particuliers, les secteurs publiques et privés, mais il donnera toujours priorité au point de vue des particuliers. Il est en effet tenu pour acquis que les données à caractère personnel – tout comme les droits et libertés fondamentaux y relatifs – méritent une protection d'une certaine qualité. Ainsi, le modèle a pour objectif de protéger les particuliers, non seulement en aidant les responsables du traitement à respecter la loi, mais aussi en allant au-delà du pur formalisme. En exigeant une justification élaborée pour chaque choix réalisé, il favorise non seulement la protection des données, mais aussi la réflexion sur les droits fondamentaux, tout en orientant le processus d'analyse vers une activité plus exhaustive que le simple contrôle de conformité qui consiste uniquement à cocher une case.

Quatrièmement, le modèle veut être facile à utiliser (convivial). En adoptant l'approche de « legal design » – un processus de conception juridique qui vise à rendre les systèmes et services juridiques davantage axés sur l'individu et plus utilisables et satisfaisants – le modèle ne guide pas seulement les évaluateurs étape par étape à travers le processus d'analyse de manière pratique, aisée et intuitive, mais il fournit aussi des instructions et des explications limitées au strict minimum nécessaire.

Cinquièmement et finalement, le modèle accepte aussi de ne pas être définitif. A la manière des cadres et des méthodes d'analyses d'impact, et pareillement aux processus d'analyse, un modèle est un « instrument vivant » qui évolue en permanence au fur et à mesure de l'expérience acquise par son utilisation. Il doit donc être révisé en conséquence.

Le modèle proposé est soumis à un certain nombre de limitations nécessaires. Premièrement, étant basé sur un processus AIPD tel que requis par le RGPD, il *ne prend pas en considération* les spécificités d'un processus AIPD comme exigées ailleurs dans l'UE, par exemple, en vertu de la Directive 2016/680 ou du Règlement relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union (2018/1725). Deuxièmement, le modèle proposé serait rarement appliqué tel quel. En effet, il devra être adapté au contexte d'utilisation, tel que le domaine de compétence, le secteur de gouvernance ou le secteur industriel.

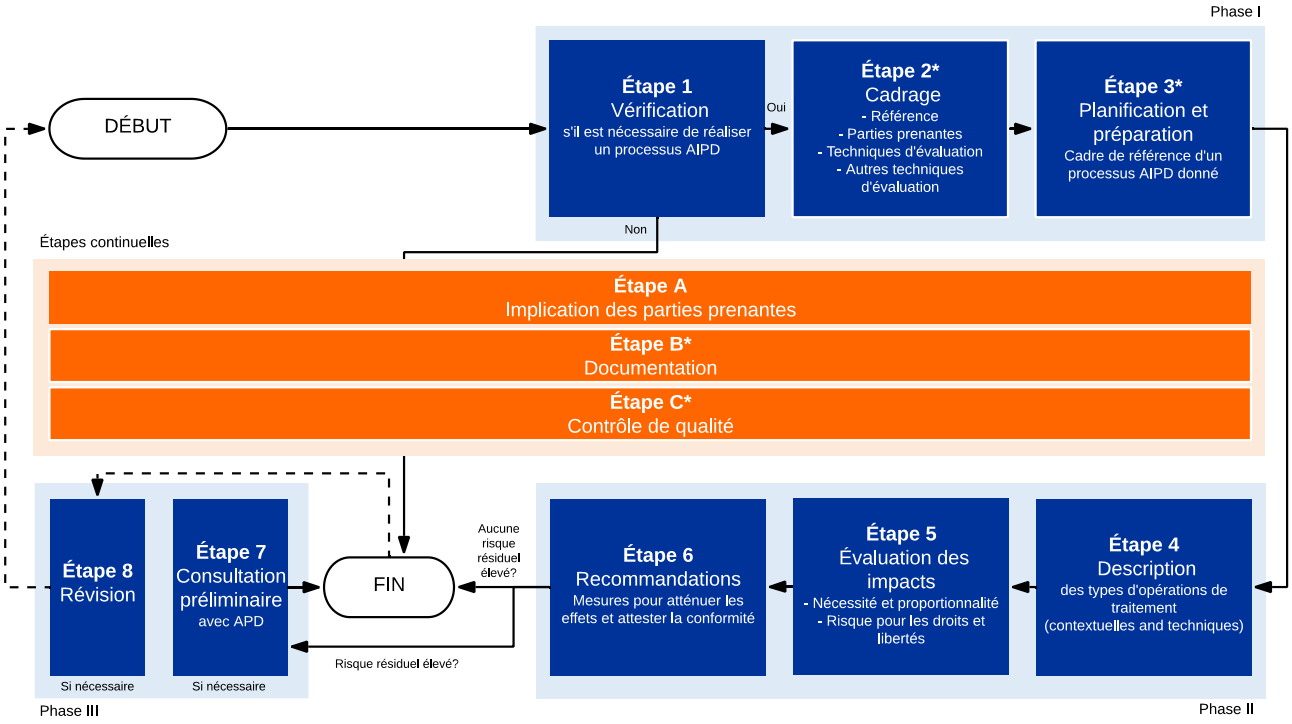
1.3 DESTINATAIRES DU MODÈLE

Le modèle proposé est tout d'abord destiné aux évaluateurs auxquels le responsable du traitement a confié la réalisation du processus AIPD. Les évaluateurs sont des personnes physiques ou morales qui exécutent le processus d'analyse dans la pratique. Le processus d'analyse est rarement une mission exécutée par une seule personne. La plupart du temps, il faudra mettre en place une équipe d'évaluateurs ayant des connaissances et expertises variées afin de mener à bien un tel processus collaboratif. Les évaluateurs peuvent être des ressources assignées en interne ou des externes travaillant contre rémunération (tels que de consultants), mais en définitive, c'est bien le responsable du traitement qui reste responsable (Article 5(2) et Article 24) et qui est tenu légalement responsable du processus d'analyse (Article 83(4)(a)). Si les responsables du traitement réalisent eux-mêmes le processus d'analyse, ils deviennent des évaluateurs.

De plus, le modèle proposé pourrait influer sur le développement de modèles d'un processus AIPD (adapté) que des autorités nationales et/ou régionales de protection des données (APD) actives au sein de l'UE et d'autres juridictions de l'Espace économique européen (EEE) pourraient émettre pour leur propre juridiction. Il peut également servir de référence à des modèles (prouvés) pour un processus AIPD dans d'autres domaines de compétences et – éventuellement – à des modèles d'autres types de processus d'analyse dans d'autres domaines de pratique.

1.4 APERÇU DE LA MÉTHODE D'ANALYSE

Le modèle proposé correspond à une méthode composée de onze étapes, dont six sont des étapes consécutives (Étapes 1–6 ; Étapes 1-3 pourraient, dans une large mesure, être exécutées en parallèle), deux des étapes « ex post » (Étapes 7-8 seront seulement déclenchées dans certaines conditions) et trois des étapes continuelles (Étapes A–C, à exécuter tout au long du processus d'analyse, parallèlement aux Étapes 1-8), groupés en quatre phases (Phases I–III ; la phase continuelle ne porte pas de numéro). L'ordre des étapes est déterminé par la manière dont chaque étape se rapporte à l'étape suivante.



1.5 MODE D'EMPLOI DU MODÈLE

Afin de réaliser le rapport du processus d'analyse, les évaluateurs complètent, dans un langage facilement compréhensible, les tableaux et/ou les champs assignés à chaque étape. Dans la mesure du possible, chaque réponse est exhaustive et suffisamment motivée (décrite, expliquée, justifiée, etc.), aussi bien pour les critères qui sont remplis que pour les critères qui ne sont pas remplis. Le cas échéant, les évaluateurs peuvent ajouter des lignes supplémentaires dans chaque tableau. Si le tableau n'offre pas assez d'espace, les évaluateurs peuvent transférer chacun des éléments vers une annexe. Alternativement, ils peuvent supprimer des tableaux et/ou des champs ; le cas échéant, les évaluateurs peuvent présenter les mêmes informations dans un autre format lorsqu'ils le jugent opportun. Les notes explicatives figurant au début de chaque étape peuvent être supprimées à la finalisation du rapport. (Parallèlement à la présente Note de Politique, d.pia.lab fournit un formulaire modifiable prêt à être utilisé.)

Suivant la méthode en 11 étapes utilisée dans ce modèle, les étapes consécutives sont marquées en bleu et les étapes continuelles en orange. Les évaluateurs complètent seulement les champs en bleu clair ou orange clair. A la fin de chaque étape, le modèle prévoit des champs où les évaluateurs peuvent, le cas échéant, noter leurs observations ou commentaires. A la réception du rapport complété par les évaluateurs, c'est au responsable du traitement de compléter les champs en vert clair seulement.

Le modèle part du principe que l'équipe des évaluateurs connaît bien le cadre juridique relative à la protection des données à caractère personnel établi par le RGPD. (Les références à des dispositions légales reprises sans autres précisions se rapportent au RGPD). Il suppose aussi qu'ils ont un minimum de connaissances du processus de l'analyse de risque et des critères limitant la jouissance des droits humain, particulièrement ceux qui ont trait à la nécessité et à la proportionnalité. Toutefois, le modèle proposé doit être lu conjointement avec les notes de politique précédentes du d.pia.lab dans lesquelles les principes fondamentaux sont expliqués en détail. D'autres références se trouvent à la fin de la présente note de politique.

Le processus AIPD est normalement initiée par le responsable du traitement ou sous la direction de celui-ci, car c'est à lui qu'incombe l'obligation de mener le processus AIPD (Article 35(1)). Si un sous-traitant a été désigné, celui-ci est obligé d'aider le responsable du traitement (Article 28(3)(f)) ; mais le sous-traitant peut aussi mener un processus d'analyse à sa propre initiative et dans le cadre de compétences qui lui est propre. Il est supposé que tous les acteurs – depuis le responsable du traitement et les évaluateurs jusqu'aux parties prenantes en passant par le délégué à la protection des données (DPD) – sont impliqués dans l'intégralité du processus d'analyse. Comme le processus d'analyse concerne des opérations de traitement de données qui, en principe, ne sont pas encore mis en place – en fait, celles-ci seront réalisées plus tard – il se peut que les évaluateurs doivent se baser sur des estimations, voire des informations incomplètes.

Nonobstant, tout a été mis en œuvre pour assurer l'exactitude des informations fournies. Il faut cependant bien se rendre compte que toutes les informations contenues dans ce document sont fournies sans garantie aucune. Ni d.pia.lab, ni les auteurs individuels, ne peuvent être tenus responsable pour les conséquences négatives qui pourraient découler de l'utilisation ou de la mauvaise utilisation de ce document, ou de la confiance témoignée au contenu de celui-ci.

UN MODÈLE DE RAPPORT DU PROCESSUS AIPD

LES ÉLÉMENTS D'IDENTIFICATION

Nom et numéro de l'initiative, s'il y a lieu	
Nom, coordonnées et autres éléments d'identification :	
▪ du/des responsable(s) du traitement	
▪ du/des sous-traitant(s), s'il y a lieu	
▪ de la/des personne(s) responsable de l'initiative (le propriétaire du projet)	
▪ de l'/des évaluateur(s)	
▪ du/des délégué(s) à la protection des données (DPD), si désigné	
▪ du responsable de la sécurité des systèmes d'information, si désigné	
▪ de l'organe compétente, supervisant la qualité de contrôle du processus d'analyse, si désigné	
▪ des autorités de protection des données (APD) compétentes	
▪ de toute autre personne impliquée, si faisable	
Version du rapport	
Niveau de confidentialité du rapport	☐ Public ☐ Confidentiel ☐ Spécifique [*Veuillez préciser*]
Date et lieu de l'élaboration du rapport	
[Tout autre détail, si faisable]	

RÉSUMÉ

[Résumez les informations les plus importantes sur le résultat de chaque étape du processus AIPD en cours.]

PHASE I : PRÉPARATION DU PROCESSUS D'ANALYSE

ÉTAPE 1 VÉRIFICATION PRÉLIMINAIRE (ANALYSE DE SEUIL)

Objectif

Le but de cette étape consiste à déterminer si le processus AIPD est nécessaire du fait qu'un ou plusieurs critères prévus par la loi ou d'autres exigences réglementaires pertinentes sont d'application ; ou, alternativement, à déterminer si le processus d'analyse n'est pas nécessaire du fait qu'une exemption est prévue.

EXTRA Le responsable du traitement peut cependant prendre l'initiative de réaliser un processus AIPD, indépendamment des exigences légales, afin de les rendre conformes aux principes de la responsabilité (Article 5(2), Article 24), de la protection des données dès la conception et de la protection des données par défaut (Article 25), et de la sécurité du traitement (Article 32).

Mise en œuvre

A partir de quelques descriptions contextuelles et techniques rudimentaires des opérations de traitement envisagées qui font l'objet de l'initiative d'analyse (voir l'*Étape 1a*), les évaluateurs étudient si les opérations en question répondent à aucun des critères de seuil (voir l'*Étape 1b*). Comme condition préalable, les évaluateurs déterminent s'il s'agit effectivement du traitement de données à caractère personnel ; si non, le RGPD n'est pas d'application et le processus AIPD n'est pas obligatoire.

Les critères sont fixés principalement par le RGPD et pourraient être complétés par un autre instrument légal ou réglementaire auquel le responsable du traitement est soumis, tel qu'un code de conduite (Article 40) (voir l'*Étape 2a*). La jurisprudence pourrait apporter des précisions supplémentaires sur ces critères.

Les informations disponibles aux premières étapes étant en principe restreintes, la description préliminaire sera succincte (environ une page) mais suffisamment détaillées pour permettre aux évaluateurs de déterminer si les critères de seuil sont remplis. Une telle description peut être basée sur les registres des opérations de traitement, pour autant que ceux-ci soient disponibles (Article 30). Les généralités sont à éviter. Si les évaluateurs déterminent que le processus d'analyse est nécessaire, cette description préliminaire sera développée plus en détail dans l'*Étape 4*.

Les critères de seuil sont basés sur la notion de risque (expliquée dans l'*Étape 5*) et sont positifs ou négatifs. (Les critères négatifs ont prévalence sur les critères positifs). Si l'un des critères positifs est rempli, le processus d'analyse sera exigé par la loi. En revanche, si l'un des critères négatifs est satisfait, le responsable du traitement est dispensé d'effectuer le processus d'analyse. Dans le premier cas, les évaluateurs passent à l'*Étape 2* du processus.

EXTRA Dans le dernier cas, les évaluateurs préparent une déclaration d'absence d'impact significatif, justifiant les raisons pour lesquelles ils ont décidé de ne pas effectuer un processus AIPD et de ne pas en poursuivre la réalisation, à moins qu'il y ait un besoin de revoir les processus d'analyse (voir l'*Étape 8*). En cas de doute, il est recommandé de mener le processus d'analyse.

ÉTAPE 1A : LE DESCRIPTION PRÉLIMINAIRE DES OPÉRATIONS DE TRAITEMENT PRÉVUES

			Explication
	Allez-vous traiter des données à caractère personnel ?		☐ Oui ☐ Non
Description contextuelle	**Nature** *(quels types d'opérations de traitement ?)*		
	Portée	Échelle *(combien ? en quelles quantités ? jusqu'à quel niveau ?)*	
		Période *(quand ? pour combien de temps ?)*	
	Contexte *(dans quelles conditions ?)*	Interne *(par rapport au responsable du traitement)*	
		Externe *(par rapport aux particuliers, aux groupes, à la société, etc.)*	
	Finalité des d'opérations de traitement *(pourquoi ?)*		
Description technique	Catégories des données à caractère personnel traités *(quoi ?)*		
	Moyens du traitement (infrastructure) *(par quels moyens ? p.ex. analogue, numérique)*		
	Flux de données envisagés (*d'où à où ? de qui à qui ?*)		
	Sécurité des données *(comment sont-elles sécurisées)*		
	Domaines de compétences/marché (*où ?*)		
	Acteurs dans la « chaîne d'approvisionnement » (*qui ?*)		
	[Autres, veuillez préciser]		

ÉTAPE 1B : VÉRIFICATION (ANALYSE DE SEUIL)

Critères positifs

Critère	*Disposition légale*	*Satisfaite ?*	*Explication*
CRITÈRE 1 : PROBABILITÉ DE RISQUE ÉLEVÉ (DE CARACTÈRE GÉNÉRAL) *Les opérations de traitement envisagées, sont-elles susceptibles d'engendrer un risque élevé pour les droits et libertés des personnes physiques ?* – critère à déterminer sur base des éléments suivants : ▪ les indicateurs de risque (nature, portée, contexte et finalités du traitement) ▪ une analyse rudimentaire des risques (*niveau de probabilité ? degré de gravité ?*) ▪ le registre des risques en matière de protection de données (si tant est qu'il en existe un) ▪ *[Autres ; veuillez préciser]*	35(1)	☐	
CRITÈRE 2 : PROBABILITÉ DE RISQUE ÉLEVÉ (DE CARACTÈRE SPÉCIFIQUE) *Les opérations de traitement envisagées, présentent-elles l'une des situations qualifiées par la loi comme étant susceptibles d'engendrer un risque élevé ?* notamment :			
▪ une évaluation systématique et approfondie d'aspects personnels de personnes physiques, basée sur un traitement automatisé, y compris le profilage, et sur base de laquelle sont prises des décisions produisant des effets juridiques à l'égard d'une personne physique ou l'affectant similairement de manière significative	35(3)(a)	☐	
▪ le traitement à grande échelle de catégories particulières de données ou de données à caractère personnel relatives à des condamnations pénales et à des infractions	35(3)(b)	☐	
▪ la surveillance systématique à grande échelle d'une zone accessible au public	35(3)(c)	☐	
CRITÈRE 3 : PROBABILITÉ DE RISQUE ÉLEVÉ (ÉNUMÉRATION POSITIVE) *Les opérations de traitement envisagées, figurent-elles dans la liste publique des opérations de traitement nécessitant un processus AIPD, établie par le(s) APD(s) ?*	35(4)	☐	
CRITÈRE 3 BIS : LES CODES DE CONDUITE APPROUVÉS *Y a-t-il un code de conduite approuvé exigeant un processus AIPD pour les opérations de traitement envisagées ?*	40	☐	
[Autres, voir l'Étape 2 ; veuillez préciser]		☐	
Est-il nécessaire de réaliser un processus AIPD ?		☐	**Oui** *[passez à l'Étape 2]*
		☐	**Non** *[passez à l'Étape 1c]*

Critères négatifs

Critère	*Disposition légale*	*Satisfaite ?*	*Explication*
CRITÈRE 4 : PROBABILITÉ DE RISQUE ÉLEVÉ (ÉNUMÉRATION NÉGATIVE) *Les opérations de traitement envisagées, figurent-elles dans la liste publique des opérations de traitement dispensées de la réalisation d'un processus AIPD, établie par le(s) APD(s) ?*	35(5)	☐	
CRITÈRE 5 : ANALYSE D'IMPACT (RÉGLEMENTAIRE) PRÉALABLE *Les opérations de traitement envisagées, ont-elles déjà fait l'objet d'un processus d'analyse antérieur ?*	35(10)	☐	
CRITÈRE 6 : DÉROGATIONS POUR DES PROFESSIONS SPÉCIFIQUES *Les opérations de traitement envisagées, concernent-elles des données à caractère personnel de patients ou de clients d'un médecin, d'un professionnel de la santé ou d'un avocat, et sont-elles dès lors ne pas considérées comme étant à grande échelle ?*	Considérant 91	☐	
CRITÈRE 6 BIS : LES CODES DE CONDUITE APPROUVÉS *Y a-t-il un code de conduite approuvé dispensant les opérations de traitement envisagées de la réalisation d'un processus AIPD ?*	40	☐	
[Autres, voir l'Étape 2 ; veuillez préciser]		☐	
Le responsable du traitement, est-il dispensé de réaliser un processus AIPD ?		☐	**Dispensé** *[passez à l'Étape 1c]*
		☐	**Pas dispensé** *[passez à l'Étape 2]*
S'il n'est pas nécessaire de réaliser un processus AIPD, peut-il être effectué volontairement ?		☐	**Oui** *[passez à l'Étape 2]*
		☐	**Non** *[passez à l'Étape 1c]*

ÉTAPE 1C : DÉCLARATION D'ABSENCE D'IMPACT SIGNIFICATIF EXTRA

[Si les critères de n° 1 à n° 3bis inclus ne sont PAS satisfaits, pourquoi les opérations de traitement envisagées sont-elles dispensées de la réalisation d'un processus AIPD ?]

COMMENTAIRES

[Explication]

ÉTAPE 2* CADRAGE

Objectif

Le but de cette étape consiste à identifier, de manière raisonnablement précise :

a) la référence, c'est-à-dire, un ensemble de règles du droit fondamental à la protection des données à caractère personnel et des libertés et droits fondamentaux y relatifs, reflétés dans le cadre juridique en vigueur ;

b) les catégories de parties prenantes, c'est-à-dire, les parties prenantes à impliquer dans les processus d'analyse et la façon dont celles-ci doivent être intégrées dans chaque étape (c.-à-d. les techniques pour inciter l'implication des parties prenantes) ;

c) les techniques d'évaluation autres que celles se rapportant à l'évaluation de la nécessité et de la proportionnalité et à l'évaluation du risque, à utiliser, le cas échéant, dans le processus d'analyse ; et

d) les autres techniques d'évaluation qui pourraient être nécessaires.

Mise en œuvre

RÉFÉRENCE. Dans le processus AIPD, la référence est constituée d'un ensemble de règles (a) du droit fondamental à la protection des données à caractère personnel et (b) d'autres libertés et droits fondamentaux impactés par les opérations de traitement envisagées (voir l'Article 1(2) ; Considérant 4). Au cours de cette étape, les évaluateurs vont tout d'abord dresser un inventaire de tous les aspects qui pourraient affecter les opérations de traitement envisagées. (Les opérations de traitement ne vont pas toutes déclencher les dispositions prévues par le RGPD et d'autres lois pertinentes). Comme ces droits sont régis par de nombreuses lois et d'autres instruments réglementaires, cet exercice va de pair avec une inventorisation du cadre juridique en vigueur dans un domaine de compétence déterminé.

PARTIES PRENANTES. Au cours de cette étape, les évaluateurs vont ensuite identifier les catégories de parties prenantes qui doivent être consultées, notamment – et premièrement – les personnes concernées (p.ex. les employés, les clients, les patients, les étudiants, les élèves ou les retraités) et/ou leurs représentants (p.ex. les organisations non-gouvernementales, les associations ou les groupes de défense). Or, ces consultations comprennent aussi d'autres personnes (et/ou leurs représentants) qui ont un impact sur ou qui sont affectées, concernées ou simplement intéressées par les opérations de traitement envisagées, ainsi que des experts. Le terme « parties prenantes » doit être compris au sens large, et la catégorie et le nombre à impliquer dans le processus sont proportionnels aux opérations de traitement. Des parties prenantes peuvent proposer d'autres parties prenantes. (Les particuliers, groupes et/ou organisations *spécifiques* à consulter sont déterminés dans l'*Étape 3*). Les parties prenantes ne sont *pas* des évaluateurs ; les premières apportent des éléments que les derniers vont ensuite prendre en compte ou rejeter.

Le RGPD place l'implication des parties prenantes (qui va généralement de la simple communication à la codécision) au milieu du spectre, à savoir au niveau de la consultation, ce qui signifie que leurs points de vue sont sollicités et pris en considération. Mais dans un processus AIPD, le responsable du traitement peut, de sa propre initiative, attribuer un niveau plus élevé à l'implication des parties prenantes.

Les techniques pour inciter l'implication des parties prenantes sont nombreuses et variées et vont de l'organisation d'événements (ateliers, groupes de discussion, jurys de citoyens) jusqu'aux sondages (entretiens, enquêtes, questionnaires structurés ou semi-structurés) en passant par des déclarations écrites.

TECHNIQUES D'ÉVALUATION. Au cours du processus AIPD, le RGPD prévoit le recours à deux types de techniques d'évaluation : (a) l'évaluation de la nécessité et de la proportionnalité (Article 35(7)(b)), et (b) l'évaluation du risque (Article 35(7)(c)). S'il s'avère que ces deux techniques n'apportent pas assez d'informations permettant la prise de décision, d'autres techniques d'évaluation peuvent être utilisées, telles que l'analyse de scénario (planification à l'aide de scénarios), la prospective technologique, ou l'analyse coûts-avantages (ACA). Le RGPD ne précise pas exactement la technique d'évaluation à privilégier, mais laisse le choix au responsable du traitement. Les techniques d'évaluation sont scientifiquement rigoureuses, juridiquement valables (c.-à-d. conformes à la loi) et réplicables (c.-à-d. qu'un auditeur ou juge pourrait vérifier les résultats en utilisant la même méthode).

AUTRES TECHNIQUES D'ÉVALUATION. Les évaluateurs peuvent recourir à d'autres techniques d'évaluation en dehors de l'AIPD, qui pourraient être nécessaires ou requises par la loi afin d'assurer, par exemple, l'exhaustivité des informations utilisées dans le processus de prise de décision. C'est notamment le cas si les opérations de traitement envisagées ont *également* un impact sur l'environnement naturel et/ou humain. Dans ce cas, il se peut que la loi exige ou rende

nécessaire la réalisation d'un processus d'évaluation des incidences sur l'environnement (EIE) en plus et en parallèle du processus AIPD. Une ACA peut être utilisé comme une technique d'évaluation autonome afin de déterminer si les opérations de traitement envisagées l'emportent sur leurs coûts.

De plus, pour des raisons d'exhaustivité et d'efficacité, il est possible d'intégrer différents types d'analyse d'impact et d'autres techniques d'évaluation, pourvu que la référence et/ou les techniques d'évaluation soient cohérentes et ne soient ni subordonnées l'une à l'autre, ni s'opposent l'une à l'autre. Les résultats d'un tel processus d'analyse intégré doivent ensuite être synthétisés.

ÉTAPE 2A : RÉFÉRENCE

Référence (1) : Les lois et réglementations applicables

	Les lois et réglementations applicables	*Disposition légale*	*Applicable ?*	*Explication*
lex generalis	Règlement Général sur la Protection des Données (RGPD)		☒	
	La (les) législation(s) nationale(s) complétant le RGPD		☒	
	La Directive « Police » 2016/680 [transposition nationale]		☐	
	[Autres, veuillez préciser]		☐	
lex specialis	La Directive «Vie privée et communications électroniques» [transposition nationale]		☐	
	Liste(s) nationale(s) d'exclusion/d'inclusion	35(4)–(5)	☐	
	Codes de conduite approuvés	40	☐	
	Certifications	42	☐	
	Décision(s) d'adéquation	45	☐	
	Règles d'entreprise contraignantes (REC)	47	☐	
	Clauses contractuelles types (CCT)	46(2)(c)–(d) 46(3)(a)	☐	
	[Autres, veuillez préciser]		☐	

autres	Règlement 2018/1725		☐	
	Normes techniques		☐	
	Politiques de protection des données		☐	
	Codes de conduite professionnelle *(p.ex. chartes éthiques, gouvernance d'entreprise, etc.)*		☐	
	Contrat(s) d'échange de données		☐	
	[Autres, veuillez préciser]		☐	

Référence (2) : Portée du processus d'analyse

	Portée du processus d'analyse		*Disposition légale*	*Applicable ?*	*Explication*
droit à la protection des données à caractère personnel	Principes de la protection des données à caractère personnel		5	☒	
	Base juridique pour le traitement		6–8	☒	
	Traitement de catégories particulières de données à caractère personnel		9–10	☐	
	Droits des personnes concernées	Transparence et informations	12–14	☒	
		Droit d'accès	15	☒	
		Droit de rectification	16	☒	
		Droit d'effacement	17	☐	
		Droit de limitation de traitement	18	☒	
		Droit à la portabilité des données	20	☐	
		Droit d'opposition	21	☐	
		Droit de ne pas être soumis à une prise de décision automatisée	22	☐	
	Obligations du responsable du traitement et du sous-traitant		24–39	☒	
	Transfert de données en dehors de l'UE/EEE		46–49	☐	
	Limitation des obligations et des droits		23	☐	
	Situations particulières de traitement		85–91	☐	
	[Autres, veuillez préciser]			☐	

autres droits fondamentaux	Vie privée et familiale, domicile et correspondance	Considérant 4	☐	
	Liberté de pensée, de conscience et de religion		☐	
	Liberté d'expression et d'information		☐	
	Liberté d'entreprise		☐	
	Droit à un recours effectif et à un procès équitable		☐	
	Diversité culturelle, religieuse et linguistique		☐	
	[Autres droits fondamentaux, veuillez préciser]	CDF	☐	
[Autres aspects de la protection des données à caractère personnel, veuillez préciser]			☐	

ÉTAPE 2B : PARTIES PRENANTES, LEUR NIVEAU D'IMPLICATION ET LES TECHNIQUES D'IMPLICATION LES CONCERNANT

Parties prenantes internes

Catégorie de partie prenante	*Impliquée ?*	*Niveau d'implication*	*Technique(s) d'implication de la partie prenante*	*Explication*
Sous-traitant(s)	☐			
Délégué(s) à la protection des données (DPD)	☐			
Destinataire(s) (Article 4(9))	☐			
Représentant(s) (Article 27)	☐			
Responsable de la sécurité des systèmes d'information	☐			
Service juridique	☐			
Employés, syndicats, contractants, etc.	☐			
[Autres, veuillez préciser]	☐			

Parties prenantes externes

Catégorie de partie prenante		*Impliquée ?*	*Niveau d'implication*	*Technique(s) d'implication de la partie prenante*	*Explication*
Personnes concernées, y compris : ▪ les mineurs ▪ les personnes vulnérables ▪ *[autres, veuillez préciser]*		☐			
Représentant(s) de la (des) personne(s) concernée(s)		☐			
Particuliers autres que les personnes concernées		☐			
Représentant(s) de particuliers autres que les personnes concernées		☐			
Tiers (Article 4(10))	secteur public	☐			
	secteur privé	☐			
Experts		☐			
Autorités de protection des données (APD)		☐			
[Toute autre personne affectée, etc., veuillez préciser]		☐			

Absence d'implication des parties prenantes

[Si les parties prenantes ne doivent pas être impliquées dans le présent processus AIPD, veuillez expliquer pourquoi il en est ainsi]

ÉTAPE 2C : TECHNIQUES D'ÉVALUATION

	Types de techniques d'évaluation	*Disposition légale*	*Applicable ?*	*Techniques particulières*	*Explication*
Obligatoire	Évaluation de la nécessité et de la proportionnalité	35(7)(b)	☒		
	Évaluation du risque (droits et libertés de personnes physiques)	35(7)(c)	☒		
	[Autres, voir l'Étape 2 ; veuillez préciser]		☐		
Supplémentaire	Évaluation du risque (sécurité des données)		☐		
	Planification à l'aide de scénarios		☐		
	Analyse coûts-avantages (ACA)		☐		
	Forces, Faiblesses, Opportunités, Menaces (FFOM)		☐		
	[Autres, veuillez préciser]		☐		

ÉTAPE 2D : AUTRES TECHNIQUES D'ÉVALUATION.

Types de techniques d'évaluation.	*Applicable ?*	*Technique(s) particulière(s)*	*Explication*
Évaluation des incidences sur l'environnement (EIE)	☐		
Étude d'impact sur la vie privée (EIVP)	☐		
Étude d'impact relative à l'éthique	☐		
Étude d'impact social	☐		
Étude d'impact relative à la santé	☐		
Évaluation du risque	☐		
Analyse coûts-avantages (ACA)	☐		
Forces, Faiblesses, Opportunités, Menaces (FFOM)	☐		
[Autres, veuillez préciser]	☐		

ANALYSE D'IMPACT INTÉGRÉE

	Explication
Éléments de la référence	
Technique(s) d'évaluation	
[Autres, veuillez préciser]	

COMMENTAIRES

[Explication]

ÉTAPE 3* PLANIFICATION ET PRÉPARATION

Objectif

Le but de cette étape consiste à déterminer le cadre de référence d'un processus AIPD donné. Cette étape indique la manière dont le processus AIPD sera réalisé et produira à cet effet un manuel écrit, lequel peut être mis à jour tout au long du processus d'analyse. Or, tous les éléments de cette étape ne sont pas d'égale importance ou applicabilité.

Mise en œuvre

DES OBJECTIFS PARTICULIERS POUR UN PROCESSUS AIPD DÉTERMINÉ. De manière générale, le but *principal* d'un processus AIPD consiste à assurer le niveau de protection le plus élevé possible aux particuliers dont les données à caractère personnel sont traitées au cours des opérations envisagées, alors que son but *formel* consiste à respecter la loi (voir l'Article 35(7)(d)). Un processus AIPD vise à répondre à ces deux objectifs en facilitant le processus de prise de décision relatif au déploiement et à la forme des opérations de traitement envisagées. Mais toujours est-il que c'est au responsable du traitement d'apporter des précisions sur les objectifs particuliers d'un processus d'analyse déterminé.

CRITÈRES D'ACCEPTABILITÉ DES IMPACTS NÉGATIFS. Le responsable du traitement détermine et justifie les critères pour l'acceptabilité des effets négatifs. Un tel seuil est fixé et motivé pour chaque technique d'évaluation utilisée (voir l'*Étape 2c*). Le responsable du traitement détermine et justifie le seuil au-dessous duquel une opération de traitement est jugée pas nécessaire et/ou disproportionnée à la lumière du contexte juridique ou culturel.

Le responsable du traitement fixe également un seuil au-dessus duquel un risque ne serait pas accepté, étant donné le contexte juridique ou culturel ou le comportement vis-à-vis du risque (p.ex. sujet au risque ou adverse au risque). En d'autres termes, le responsable du traitement spécifie le niveau de risque qui est acceptable. A cet effet, il définit à l'avance tant les échelles de probabilité (vraisemblance) et que celles de gravité.

RESSOURCES À ENGAGER. Le responsable du traitement identifie et assure la disponibilité de suffisamment de ressources pour réaliser le processus AIPD. Celles-ci comprennent, mais sans y être limitées : le temps (heures, jours ou mois à consacrer à la réalisation du processus AIPD dans son intégralité) ; l'argent (coût du travail, équipement, implication des parties prenantes, etc.) ; les effectifs (nombre de personnes à affecter au processus AIPD, à temps partiel ou à temps plein) ; les connaissances (expertise des évaluateurs, notamment en matière de législation, d'éthique, de données, d'informatique, de gestion de projet, de relations publiques, etc.) ; l'expertise (expérience requise par les personnes affectées au processus AIPD) ; les locaux (lieu(x) où le processus AIPD sera réalisé) et l'infrastructure (les moyens nécessaires pour la réalisation du processus AIPD, p.ex. le matériel informatique et les logiciels). Les évaluateurs peuvent recourir à des logiciels permettant l'automatisation de certains éléments du processus, ce qui pourrait leur faciliter le travail.

PROCÉDURES ET CALENDRIER. Le responsable du traitement détermine le calendrier du processus AIPD notamment en spécifiant les étapes importantes et les délais, et en attribuant des responsabilités aux évaluateurs, tout en précisant qui est responsable devant qui au sein de la structure organisationnelle.

LES ÉVALUATEURS (L'ÉQUIPE D'ÉVALUATEURS), LEURS RÔLES ET RESPONSABILITÉS. La réalisation d'un processus d'analyse nécessite plusieurs types d'expertise. Le responsable du traitement, tout en se basant sur des critères transparents, sélectionne les évaluateurs, soit en interne, soit en externe (la mission est alors externalisée), soit en combinant des ressources internes et externes. L'équipe des évaluateurs peut être modifiée et/ou élargie au fur et à mesure que le processus d'analyse progresse. Si le processus d'analyse est externalisé, entièrement ou en partie, le responsable du traitement conclut un contrat de service avec les évaluateurs externes. Le responsable du traitement définit clairement leurs rôles et responsabilités (notamment en spécifiant la personne dont les évaluateurs relèvent directement), et se porte garant de leur indépendance professionnelle (p.ex. les évaluateurs ne sollicitent, ni ne reçoivent des instructions ; leur partis pris sont clairement indiqués comme tels).

PARTIES PRENANTES. En se fondant sur les catégories prédéfinies dans l'*Étape 2b*, les évaluateurs identifient les parties prenantes de manière à assurer leur diversité (notamment en termes de parité hommes-femmes, de répartition géographique, d'âge ou de multidisciplinarité) ainsi que leurs coordonnées si des techniques d'implication directe des parties prenantes sont utilisées. En fonction de sa longueur, la liste peut être complétée dans le modèle même ou être annexé à celui-ci. Pour des consultations à large échelle, il pourrait être opportun de prévoir un plan de consultation. Les données à caractère personnel des parties prenantes identifiées sont adéquatement protégées.

CONTINUITÉ. Le responsable du traitement spécifie la manière dont la continuité du processus d'analyse sera assurée, p.ex. dans le cas d'une réorganisation au niveau des acteurs impliqués dans le processus d'analyse (p.ex. changement du responsable du traitement, des sous-traitants, des évaluateurs, etc.), ou dans le cas de perturbations, de catastrophes naturelles ou de pannes des services publics.

RÉVISION. Le responsable du traitement spécifie les critères qui vont déclencher la révision du processus AIPD. Dans ce contexte, le RGPD prévoit, à tout le moins, une modification du niveau de risque (voir l'Article 35(11)) (voir aussi l'*Étape 8*).

ÉTAPE 3A : OBJECTIFS DU PROCESSUS D'ANALYSE

Objectif	*Applicable ?*	*Explication*
Protection de particuliers	☒	
Conformité avec la loi	☒	
[Autres, veuillez préciser]	☐	

ÉTAPE 3B : CRITÈRES POUR L'ACCEPTABILITÉ DES EFFETS NÉGATIFS

Technique d'évaluation		*Explication*
Nécessité et proportionnalité (Article 35(7)(b))		
EXTRA Critères relatifs à la limitation des droits humains (Article 52(1) CDF)		
Évaluation du risque (qualitative, quantitative) (*critères de risque*)	Échelle de probabilité	
	Échelle de gravité	
	Point d'acceptabilité	
[Autres, veuillez préciser]		

ÉTAPE 3C : RESSOURCES À ENGAGER

	Valeur	*Explication*
Temps *(pour combien de temps ?)*		
Argent *(combien ?)*		
Effectifs *(combien de personnes ?)*		
Connaissances *(quelle expertise ?)*		
Savoir-faire *(quelle expérience ?)*		
Locaux *(où ?)*		
Infrastructure *(par quels moyens ?)*		
[Autres, veuillez préciser]		

ÉTAPE 3D : PROCÉDURES ET CALENDRIER DU PROCESSUS D'ÉVALUATION

	Étapes importantes	*Délais*	*Responsabilité*	*Supervision*
1	*[Veuillez préciser]*			
2				

ÉTAPE 3E : ÉVALUATEURS, RÔLES ET RESPONSABILITÉS

	Nom	*Si externe : organisation*	*Coordonnées*	*Expertise*	*Rôles et responsabilités*	*Autres informations*
1	*[Veuillez préciser]*				*[Directeur]*	
2						

ÉTAPE 3F : PARTIES PRENANTES

[Veuillez fournir les coordonnées de toutes les parties prenantes qui seront impliquées dans la réalisation du présent processus AIPD et, le cas échéant, le plan de consultation.]

ÉTAPE 3G : CONTINUITÉ DU PROCESSUS D'ANALYSE

[Comment la continuité du présent processus d'analyse sera-t-elle assurée au niveau du responsable du traitement en cas de perturbation, de réorganisation, etc. ?]

ÉTAPE 3H : CRITÈRES DÉCLENCHANT LA RÉVISION DU PROCESSUS AIPD

Critère	*Applicable ?*	*Explication*
Modification de la probabilité et/ou de la gravité d'un risque	☒	
[Autres, veuillez préciser]	☐	

COMMENTAIRES

[Explication]

ÉTAPES CONTINUELLES DE LA PHASE I

ÉTAPE A IMPLICATION DES PARTIES PRENANTES

Objectif

Le but de cette étape continuelle consiste à consulter, tout au long du processus, les personnes concernées et/ou leurs représentants, ce qui revient à demander leur avis sur les opérations de traitement envisagées, à moins si cela est possible dans la pratique (Article 35(9)).

EXTRA De plus, les évaluateurs pourraient décider d'impliquer d'autres parties prenantes à un niveau plus large.

Mise en œuvre

Les parties prenantes sont identifiées, informées, impliquées (consultées) et leurs avis sont, en fin de compte, pris en considération.

Les parties prenantes dont les catégories ont été déterminées dans l'*Étape 2b* sont identifiées plus en détail dans l'*Étape 3f*. Leur implication est continue et leur avis sur le sujet examiné est demandé à chaque étape. (Leur implication est regroupée *par phase* du processus d'analyse).

Les informations fournies et recherchées sont solides, précises et significatives. Les informations données aux parties prenantes sont rédigées dans un langage clair et pourraient nécessiter la préparation de documentation spécifique, telle que des exposés techniques. Les parties prenantes sont impliquées tout en respectant les obligations de confidentialité, à savoir les secrets d'état, les secrets commerciaux, les données à caractère personnel ou autres informations privilégiées.

Les évaluateurs examinent les points de vue recueillis auprès des parties prenantes et prennent position par rapport à leurs avis, c.-à-d. qu'ils les acceptent ou non. Dans ce dernier cas, les évaluateurs exposent de manière exhaustive les raisons qui ont motivé ce rejet.

L'implication des parties prenantes et le contrôle de qualité (voir l'*Étape B*) sont spécifiés après la conclusion de chaque phase du processus d'analyse. Après la première phase, les évaluateurs et les organes responsables du contrôle de qualité cherchent à savoir si la décision de réaliser un processus AIPD était justifiée et, s'il en est ainsi, si la portée du processus d'analyse et le cadre de référence étaient également corrects. Après la deuxième phase, ils tiennent à savoir si les effets ont été évalués de manière correcte. Après la troisième phase, ils sont intéressés à savoir si les risques résiduels ont été évalués de manière correcte et/ou si le processus d'analyse doit être effectué à nouveau.

	Partie(s) prenante(s) identifiée(s)	*Quelles sont les informations communiquées aux parties prenantes ?*	*Quel retour les parties prenantes ont-elles donné (p.ex. une opinion) ?*	*Comment ce retour a-t-il été intégré ? Pourquoi a-t-il été rejeté ?*
interne	Sous-traitant(s)			
	Délégué(s) à la protection des données (DPD)			
	Destinataire(s) (Article 4(9))			
	Représentant(s) (Article 27)			
	Responsable de la sécurité des systèmes d'information			

	Service juridique				
	Employés, syndicats, contractants, etc.				
	[Autres, veuillez préciser]				
externe	Personne(s) concernée(s)				
	Représentant(s) de la (des) personne(s) concernée(s)				
	Particuliers autres que les personnes concernées				
	Représentant(s) de particuliers autres que les personnes concernées				
	Tiers (Article 4(10)) — secteur public				
	Tiers (Article 4(10)) — secteur privé				
	Experts				
	Autorités de protection des données (APD)				
	[Autres, veuillez préciser]				

Absence d'implication des parties prenantes dans la présente phase

[Si les parties prenantes ne sont pas impliquées dans la présente phase du processus AIPD, veuillez expliquer pourquoi il en est ainsi.]

ÉTAPE B* CONTRÔLE DE QUALITÉ

Objectif

Le but de cette étape continuelle consiste à vérifier, en interne et/ou en externe, et tout au long du processus d'analyse, si celui-ci est conforme à une norme de performance déterminée et, le cas échéant, à remédier à toute irrégularité.

Mise en œuvre

Le contrôle de qualité peut être interne, externe, ou interne et externe, et prendre la forme d'un suivi, d'une révision, d'un audit, etc. Le responsable du traitement pourrait exiger que l'équipe des évaluateurs soit mise au courant sur les progrès du processus d'analyse, soit régulièrement, soit ponctuellement. Il pourrait également mettre en place un outil permettant le suivi du progrès ou un conseil consultatif interne. (L'indépendance professionnelle des évaluateurs reste garantie). En parallèle, le DPD doit aussi surveiller le processus AIPD et donner des conseils à ce sujet. Le contrôle de qualité externe peut être effectué par une organisation d'audit engagée par le responsable du traitement, ou, alternativement, par une APD ; il peut être réalisé à la demande du responsable du traitement, ou d'office (p.ex. lorsque la loi l'exige).

Le contrôle de qualité peut être structuré, permanent (récurrent dans toutes les étapes du processus) ou ponctuel ; il peut être formel (c.-à-d. qu'il vérifie si le processus est conforme aux procédures propres au processus AIPD) ou substantif (c.-à-d. qu'il vérifie si les risques ont été évalués de manière appropriée) ; il peut être réalisé au cours du processus ou après celui-ci. Dans le cas d'une action en justice, ce sont les tribunaux qui vont réviser le processus AIPD, soit au niveau de sa forme, soit au niveau de son contenu, soit au niveau de sa forme et de son contenu.

Organe de contrôle de qualité.	*Quel est le retour qui a été reçu ?*	*Comment ce retour a-t-il été implémenté ? Pourquoi a-t-il été rejeté ?*
Délégué(s) à la protection des données (DPD)		
Autorités de protection des données (APD)		
[Autres, veuillez préciser]		

Absence de contrôle de qualité dans la présente phase

[Si la qualité n'a pas été contrôlée dans la présente phase du processus AIPD, veuillez expliquer pourquoi il en est ainsi]

COMMENTAIRES

[Explication]

PHASE II : ÉVALUATION

ÉTAPE 4 DESCRIPTION SYSTÉMATIQUE

Objectifs

Le but de cette étape constitue à donner, à travers une extension de la description préliminaire, une description systématique des opérations de traitement envisagées, tant sur le plan contextuel que technique.

Mise en œuvre

La description systématique concerne donc tant les aspects contextuels que les aspects techniques des opérations de traitement envisagées, ainsi que toutes les autres informations utiles. Les aspects contextuels portent sur la nature (les caractéristiques inhérentes), la portée (la dimension et l'envergure, p.ex. en termes de durée, de budget, de complexité, etc.) et les fins (les objectifs) des opérations de traitement envisagées, et, le cas échéant, l'intérêt légitime poursuivi par le responsable du traitement. La description peut être accompagnée d'un diagramme de flux de données et/ou d'autres visualisations, à joindre en annexe. Elle peut être basée sur les registres des opérations de traitement (Article 30). Les généralités sont à éviter. La description peut subir des modifications à mesure que le processus d'analyse progresse.

La description systématique développe plus en détail la description préliminaire (voir l'*Étape 1a*) et sera donc bien plus étendue que celle-ci. Puisqu'elle constitue la base de l'analyse d'impact de l'*Étape 5*, elle est suffisamment complète, précise et fiable.

UNE DESCRIPTION SUCCINCTE DE L'INITIATIVE PRÉVUE

[Explication]

UNE DESCRIPTION DÉTAILLÉE DE L'INITIATIVE PRÉVUE

				Explication
Description contextuelle	**Nature** *(quels types d'opérations de traitement ? P.ex. collecte, stockage, effacement, etc.)*		1	
			2	
			…	
	Portée	Échelle *(combien ? en quelles quantités ? jusqu'à quel niveau ?)*		
		Période *(quand ? pour combien de temps ?)*		
	Contexte *(dans quelles conditions ?)*	Interne *(par rapport au responsable du traitement)*		
		Externe *(par rapport aux particuliers, aux groupes, à la société, etc.)*		
	Finalité des d'opérations de traitement, y compris, le cas échéant, l'intérêt légitime *(pourquoi ?)*			
	EXTRA **Avantages** des d'opérations de traitement	pour les particuliers, y compris les personnes concernées		
		pour le responsable du traitement		
		pour la société dans son ensemble		
	EXTRA **Inconvénients** des opérations de traitement	pour les particuliers, y compris les personnes concernées		
		pour le responsable du traitement		
		pour la société dans son ensemble		

Description technique	Catégories des données à caractère personnel *(quoi ?)* ▪ *catégories particulières de données à caractère personnel* ▪ *données à caractère personnel de personnes vulnérables (p.ex. les enfants)* ▪ *données de nature très personnelle*	
	Moyens du traitement (infrastructure) *(par quels moyens ?)*	
	Flux de données envisagés *(d'où à où ? de qui à qui ?)*	
	Sécurité des données *(comment sont-elles sécurisées)*	
	Domaines de compétences/marché *(où ?)*	
	Acteurs dans la « chaîne d'approvisionnement » *(qui ?)*	
	[Autres, veuillez préciser]	

DIAGRAMME DE FLUX DES DONNÉES (À CARACTÈRE PERSONNEL) ET/OU AUTRES VISUALISATIONS

[Veuillez insérer un diagramme]

COMMENTAIRES

[Explication]

ÉTAPE 5 ÉVALUATION DES IMPACTS

Objectifs

Le but de cette étape consiste à évaluer la nécessité et la proportionnalité des opérations de traitement envisagées au regard de leur finalité, et à évaluer les risques aux droits et libertés des particuliers découlant de celles-ci.

Mise en œuvre

A cet effet, les évaluateurs utilisent les techniques d'évaluation prédéfinies dans l'*Étape 2c* et fondent leur analyse sur les résultats obtenus dans l'*Étape 4*. Les évaluateurs peuvent recourir à l'une des quelques rares méthodes adéquates jusqu'à présent disponibles, ou utiliser la méthode proposée dans le présent modèle. Contrairement aux méthodes utilisées pour l'évaluation du risque (notamment les normes internationales telle que les normes ISO 31000:2018 ou ISO 27005:2018), les méthodes destinées à évaluer la proportionnalité et la nécessité dans le contexte de la protection des données à caractère personnel sont plutôt rares.

ÉVALUATION DE LA NÉCESSITÉ ET DE LA PROPORTIONNALITÉ. L'évaluation de la nécessité et de la proportionnalité peut s'effectuer à deux niveaux. Premièrement, chaque opération de traitement de données est évaluée par rapport aux principes de la protection des données à caractère personnel (voir le niveau 1). Il s'agit notamment de : la licéité, l'impartialité et la transparence, la limitation des finalités, la minimisation des données, l'exactitude, la limitation de la conservation, l'intégrité et la confidentialité (Article 5(1), y compris la sécurité du traitement (Article 32)) et la protection des données dès la conception et la protection des données par défaut (Article 25). Chaque opération de traitement de données est évaluée dans un tableau spécifique, à reproduire pour chaque opération de traitement de données.

EXTRA Étant donné qu'un droit fondamental est en jeu, et considérant qu'un processus d'analyse des opérations de traitement envisagées réalisé à la lumière des seuls principes de protection des données à caractère personnel (niveau 1) pourrait dans certains cas ne pas être suffisamment exhaustif et être au détriment du niveau de protection et de la qualité du processus de prise de décision qu'il est supposé faciliter, les évaluateurs pourraient étendre leur évaluation à l'ensemble des critères relatifs à la limitation des droits humains. En d'autres termes, alors qu'il est supposé que toutes les dispositions du RGPD, et particulièrement les principes relatifs à la protection des données à caractère personnel, soient destinées à respecter les critères de la limitation de l'exercice des droits humains (Article 52(1) de la Charte des Droits Humains de l'UE (CDF)) (niveau 1), il pourrait encore y avoir des instances qui mettent en doute l'existence d'une telle hypothèse. Pour cette raison, l'initiative envisagée qui fait l'objet de l'analyse, doit être étudiée en fonction de l'ensemble de ces critères de limitation. Par exemple, malgré la présomption de conformité avec les droits fondamentaux, une disposition du RGPD pourrait, entièrement ou en partie, y être contraire ; il pourrait en aller de même d'une exemption ou d'une dérogation nationale au RGPD (p.ex. le traitement à des fins journalistiques et à des fins d'expression universitaire, artistique ou littéraire ; Article 85). Une telle évaluation plus large pourrait cependant s'appliquer seulement à certaines catégories d'évaluateurs et/ou à des opérations particulières de traitement de données (p.ex. une mission réalisée pour des raisons d'intérêt public).

Puisque le droit à la protection des données à caractère personnel et la majorité des droits fondamentaux y afférant ne sont pas absolus mais plutôt relatifs (une atteinte à un droit ne peut se justifier que dans certaines conditions), les cinq critères de limitation définies dans l'Article 52 CDF peuvent être interprétés comme suit :

- *légalité* (c.-à-d. que le fondement pour réaliser une opération de traitement de données est « prévu par la loi » qui est de qualité suffisante, notamment en termes de clarté, d'accessibilité, de précision, de prévisibilité ou de conformité avec les règles de l'État de droit) ;
- le respect du contenu essentiel d'un droit (c.-à-d. que l'atteinte à un droit fondamental n'empêche pas l'exercice d'un droit) ;
- *légitimité* (c.-à-d. que l'opération de traitement sert soit un « intérêt général » déterminé (voir aussi l'Article 3 du Traité sur l'Union européenne (TUE)) soit la « protection des droits et libertés d'autrui ») ;
- *nécessité* (c.-à-d. que l'opération de traitement est nécessaire et répond réellement aux objectifs légitimes) ; et
- *proportionnalité au sens strict* (p.ex. équilibrage) (c.-à-d. que l'option la moins intrusive a été sélectionnée).

De plus, il est soutenu en vertu de la doctrine que *l'adéquation* d'une opération de traitement devrait également être évaluée, c.-à-d. qu'il faudrait examiner si une opération de traitement déterminée est adaptée et permet donc d'atteindre un objectif légitime.

En vertu de l'Article 52(3) CDF, le « sens et la portée » des droits, y compris leur critères de limitation, « sont les mêmes que ceux que leur confère » la Convention européenne des droits de l'Homme (CEDH).

ÉVALUATION DU RISQUE. Sur la base du RGPD, on entend par risque une conséquence négative résultant d'opérations de traitement qui pourrait ou non se produire à l'avenir. Si une telle conséquence se matérialise, elle pourrait causer des dommages physiques, matériels ou non-matériels, *non seulement* aux responsables du traitement ou sous-traitants, mais également aux personnes physiques (essentiellement aux personnes concernées). L'évaluation du risque doit être aussi objective que possible (Considérants 75–76). Or, cette ambition n'est pas toujours réalisable dans la pratique, à cause d'ambiguïtés sur les probabilités attribuables et les potentiels types de dommages, et parce qu'on prend en compte des perceptions de risque « subjectives » des parties prenantes (p.ex. les personnes concernées).

Un risque s'évalue généralement en combinant deux mesures, notamment sa vraisemblance ou sa probabilité (c.-à-d. la chance qu'il se produise) et sa gravité (c.-à-d. la magnitude des conséquences) (voir Considérant 76). Un risque peut être évalué de manière qualitative ou quantitative, ou en combinant ces deux méthodes. Certains aspects de la protection des données à caractère personnel s'inscrivent dans la gestion qualitative du risque, tels que le risque d'atteinte aux droits et libertés ; alors que d'autres rentrent dans la gestion quantitative, tels que la sécurité des données. L'évaluation quantitative du risque mesure la probabilité d'occurrence d'un risque en associant cette probabilité à la gravité du risque. La probabilité est mesurée sur une échelle allant de 0 à 1. Quant à l'évaluation qualitative de risque, celle-ci utilise les niveaux de vraisemblance du risque, exprimés par le biais d'une échelle descriptive à quatre échelons allant de négligeable, fiable, moyen et élevé, combinés à la gravité du risque. Enfin, la gravité d'un risque indique l'ampleur du dommage dans le cas où le risque se matérialiserait. La gravité est également indiquée par le biais d'une échelle descriptive à quatre échelons. Les deux échelles – celle de la vraisemblance et celle de la gravité – sont prédéfinies et motivées dans l'*Étape 3b*.

Une méthode d'évaluation de risque traditionnelle exige, premièrement, l'identification d'un risque, c.-à-d. qu'elle commence par le localiser, le reconnaître et le décrire. (Dans ce cas, il pourrait être utile de recourir à des bases de connaissance). La deuxième étape consiste à analyser le risque, ce qui revient à appréhender sa nature afin de déterminer le niveau de risque, notamment en multipliant la vraisemblance (la probabilité) de son occurrence par la gravité de ses conséquences. La troisième étape comporte l'évaluation de risque, c.-à-d. que les résultats de l'évaluation de risque sont comparés aux critères de risque (voir l'*Étape 3b*) afin de déterminer si le risque et son niveau sont acceptables, si des mesures d'atténuation du risque sont recommandées et s'il y a un risque auquel il faut accorder priorité. (Le traitement du risque se trouve en dehors du périmètre du processus d'évaluation du risque, et constitue donc un processus séparé).

ÉTAPE 6 RECOMMANDATIONS

Objectif

Le but de cette étape consiste à suggérer des mesures permettant de traiter les risques, la non-nécessité et la disproportionnalité des opérations de traitement identifiées dans l'étape précédente afin de protéger les particuliers et de se conformer à la loi, « compte tenu des droits et des intérêts légitimes des personnes concernées et des autres personnes affectées » (Article 35(7)(d)).

EXTRA Les évaluateurs pourraient suggérer des mesures pour maximiser les effets positifs.

Mise en œuvre

Les évaluateurs recommandent et décrivent les mesures d'atténuation pour chaque effet négatif (risques, interférences disproportionnées et non-nécessaires) identifié dans l'*Étape 5*. Les recommandations proposées concernent les moyens (obligation de moyens) en non pas les résultats.

Pour chaque principe relatif à la protection des données à caractère personnel (niveau 1) et/ou critère de limitation des droits humains (niveau 2) qui n'ont *pas* été satisfaits dans l'étape précédente, les évaluateurs recommandent des mesures en vue de répondre à ces principes et/ou critères.

Chaque risque est atténué en modifiant soit sa vraisemblance (sa probabilité) (en limitant l'exposition au risque, par exemple), soit sa gravité (en élaborant un plan d'action dans le cas où le risque se produirait, par exemple), soit sa vraisemblance (sa probabilité) et sa gravité. Les risques peuvent être évités, atténués, transférés (dans le temps, ou à une autre entité, telle qu'une société externe ou une compagnie d'assurance, etc.), ou acceptés. Un risque résiduel est

un risque qui perdure s'il n'y a pas de mesure disponible pour l'atténuer. Il déclenche une consultation préalable avec une APD (voir l'*Étape 7*).

Tant pour le risque que pour la non-nécessité et la disproportionnalité, les mesures d'atténuation peuvent être de nature réglementaire (légale), technique, organisationnelle ou comportementale. (Dans ce cas, il pourrait être utile de recourir à des bases de connaissance). Les évaluateurs pourraient d'abord dresser le bilan des mesures déjà prévues ou mises en place. Ils terminent cette étape par un plan d'implémentation spécifiant la personne responsable et le délai et de la mise en œuvre de chaque mesure.

A la réception du rapport, la direction du responsable du traitement prend une décision par rapport au déploiement de l'initiative envisagée. Si elle décide d'aller de l'avant, elle détermine également les conditions auxquelles ce déploiement aura lieu. Plus concrètement, après avoir reçu le rapport, la direction du responsable du traitement prend position sur chacune de recommandations proposées par les évaluateurs. Si la direction rejette ou modifie l'une de recommandations, elle doit motiver sa décision de manière circonstanciée. Avec l'accord du responsable du traitement, certaines des recommandations peuvent déjà être mises en œuvre au cours du processus d'analyse.

NÉCESSITÉ ET PROPORTIONNALITÉ DES OPÉRATIONS DE TRAITEMENT

Niveau 1 : Principes de la protection des données à caractère personnel

Identifiant de l'opération de traitement	
Type d'opération de traitement	

ÉTAPE 5 ÉVALUATION DES EFFETS | **ÉTAPE 6 RECOMMANDATIONS**

Principe		*Disposition légale*	*Applicable ?*	*Satisfaite ?*	*Explication*	*Plan d'action si principe pas satisfaite*				
						Mesures mises en place	*Mesures à mettre en place*	*Personne responsable*	*Priorité*	*Délais*
Licéité	Consentement	6(1)(a)	☐	☐						
	Contrat	6(1)(b)	☐	☐						
	Respect d'une obligation légale	6(1)(c)	☐	☐						
	Intérêts vitaux	6(1)(d)	☐	☐						

	Intérêt public	6(1)(e)	☐	☐						
	Intérêts légitimes	6(1)(f)	☐	☐						
Loyauté		5(1)(a)		☐						
Transparence				☐						
Limitation des finalités	Déterminé	5(1)(b)		☐						
	Explicite			☐						
	Légitime			☐						
	Ne font pas objet d'un traitement ultérieur			☐						
	(Exceptions)	89(1)		☐						
Minimisation des données	Adéquate	5(1)(c)		☐						

	Pertinente		☐						
	Limitée		☐						
Exactitude	Exact	5(1)(d)	☐						
	Tenu à jour		☐						
Limitation de la conservation	Requise	5(1)(e)	☐						
	(Exceptions)	89(1)	☐						
Sécurité des données	Intégrité et confidentialité	5(1)(f)	☐						
	Sécurité du traitement	32	☐						
Protection des données dès la conception		25(1)	☐						
Protection des données par défaut		25(2)	☐						

Niveau 2 : Critères relatifs à la limitation des droits humains (Article 52(1) CDF) EXTRA

ÉTAPE 5 ÉVALUATION DES EFFETS			ÉTAPE 6 RECOMMANDATIONS				
			Plan d'action si principe pas satisfait				
Critère	*Satisfait ?*	*Explication*	*Mesures mises en place*	*Mesures à mettre en place*	*Personne responsable*	*Priorité*	*Délais*
LÉGALITÉ *L'initiative envisagée prévue par la loi, est-elle de qualité suffisante ?*	☐						
CONTENU ESSENTIEL *L'initiative envisagée, permet-elle encore l'exercice d'un droit fondamental ou d'une liberté fondamentale ?*	☐						
PROPORTIONNALITÉ LÉGITIMITÉ *L'initiative envisagée, sert-elle un objectif légitime ?*	☐						

ADÉQUATION *L'initiative envisagée, est-elle adaptée pour et permet-elle d'atteindre cet objectif ?*	☐						
NÉCESSITÉ *L'initiative envisagée, est-elle nécessaire pour atteindre cet objectif ?*	☐						
LA PROPORTIONNALITÉ AU SENS STRICT (BALANCEMENT) *L'atteinte au droit, est-elle justifiée par rapport au gain réalisé pour la protection du droit ou de l'intérêt concurrent ?*	☐						

RISQUE POUR LES DROITS ET LIBERTÉS DE PERSONNES PHYSIQUES

ÉTAPE 5 ÉVALUATION DES EFFETS							**ÉTAPE 6 RECOMMANDATIONS**								
IDENTIFICATION DU RISQUE		ANALYSE DU RISQUE					ÉVALUATION DU RISQUE								
							Réponse au risque					*Plan d'action*			
Identifiant	*Risque*	*Description (source du risque, propriétaire du risque, etc.)*	*Vraisemblance (probabilité) d' occurrence* V[P]	*Gravité de la (des) conséquence(s) si le risque se produit* G	*Niveau de risque (score)* R = V[P] * G	*Explication*	*Type*	*Description*	*Risque révisé niveau (score) (Y a-t-il aucun risque résiduel ?)* [V]P	G	R	*Mesures mises en place*	*Mesures à mettre en place*	*Personne responsable*	*Priorité*	*Délais*
1	*[Veuillez préciser]*														
2															
3															
4															

Matrice des risques

Avant recommandations	*Après recommandations*
[Veuillez insérer un diagramme]	*[Veuillez insérer un diagramme]*

AUTRES TECHNIQUES D'ÉVALUATION EXTRA

Évaluation	*Recommandations.*
[Explication]	*[Explication]*

RECOMMANDATIONS

	Synthèse des recommandations	*Décision du responsable du traitement et justification de sa décision*
1	*[Explication]*	
2		

	Recommandation générale		*Décision du responsable du traitement et justification de sa décision*
☐	déployer l'initiative telle quelle		
☐	modifier l'initiative	*[Veuillez préciser comment]*	
☐	annuler l'initiative	*[Veuillez préciser pourquoi]*	

COMMENTAIRES

[Explication]

ÉTAPES CONTINUELLES DE LA PHASE II

ÉTAPE A IMPLICATION DES PARTIES PRENANTES

	Partie(s) prenante(s) identifiée(s)		*Quelles sont les informations communiquées aux parties prenantes ?*	*Quel retour les parties prenantes ont-elles donné (p.ex. une opinion) ?*	*Comment ce retour a-t-il été intégré ? Pourquoi a-t-il été rejeté ?*
interne	Sous-traitant(s)				
	Délégué(s) à la protection des données (DPD)				
	Destinataire(s) (Article 4(9))				
	Représentant(s) (Article 27)				
	Responsable de la sécurité des systèmes d'information				
	Service juridique				
	Employés, syndicats, contractants, etc.				
	[Autres, veuillez préciser]				
externe	Personne(s) concernée(s)				
	Représentant(s) de la (des) personne(s) concernée(s)				
	Particuliers autres que les personnes concernées				
	Représentant(s) de particuliers autres que les personnes concernées				
	Tiers (Article 4(10))	secteur public			
		secteur privé			
	Experts				
	Autorités de protection des données (APD)				

	[Autres, veuillez préciser]			

Absence d'implication des parties prenantes dans la présente phase

[Si les parties prenantes ne sont pas impliquées dans la présente phase du processus AIPD, veuillez expliquer pourquoi il en est ainsi.]

ÉTAPE B* CONTRÔLE DE QUALITÉ

Organe de contrôle de qualité.	*Quel retour a été reçu ?*	*Comment ce retour a-t-il été implémenté ?* *Pourquoi a-t-il été rejeté ?*
Délégué(s) à la protection des données (DPD)		
Autorités de protection des données (APD)		
[Autres, veuillez préciser]		

Absence de contrôle de qualité dans la présente phase

[Si la qualité n'a pas été contrôlée dans la présente phase du processus AIPD, veuillez expliquer pourquoi il en est ainsi]

COMMENTAIRES

[Explication]

PHASE III : ÉTAPES *EX POST*

ÉTAPE 7 CONSULTATION PRÉALABLE AUPRÈS D'UNE AUTORITÉ DE CONTRÔLE

Objectif

Le but de cette étape consiste à demander l'avis d'une autorité de contrôle lorsque le processus AIPD indique que le traitement présenterait un (des) risque(s) résiduel(s) élevé(s) si le responsable du traitement ne prend pas de mesures pour atténuer le risque (Article 36).

Mise en œuvre

Beaucoup d'APDs demandent des formulaires (modèles) spécifiques pour solliciter une consultation préalable. Le Comité Européen de la Protection des Données (CEPD) tient une liste de contact actualisée de tous ses Membres APD.

Lorsque l'APD est d'avis que les opérations de traitement envisagées constitueraient une violation au RGPD, elle fournit un avis écrit au responsable du traitement dans un délai maximum de 8 semaines. Ce délai peut être prolongé de 6 semaines, en fonction de la complexité de la demande. Le cas échéant, l'APD peut demander au responsable du traitement de fournir des informations supplémentaires, auquel cas les délais mentionnés ci-dessus seront suspendus. Une APD peut également faire usage de ses pouvoirs visés à l'Article 58.

APD(s) compétente(s)	
Date de soumission	
Date de réception de la réponse	
Demande (résumé)	
Réponse (résumé)	
Décision du responsable du traitement après consultation	

COMMENTAIRES

[Explication]

ÉTAPE 8 RÉVISION

Objectif

Le but de cette étape consiste à décider si et quand un processus AIPD doit être refait, entièrement ou en partie, après le déploiement des opérations de traitement envisagées.

Mise en œuvre

Selon les critères définis dans l'*Étape 3h*, le responsable du traitement revoit le processus AIPD lorsque c'est nécessaire et, à tout le moins, lorsqu'il se produit une modification du risque présenté par les opérations de traitement, c.-à-d., lorsque la nature, la portée, le contexte ou la finalité des opérations de traitement ont changé, entraînant de la sorte un changement du niveau de risque (Article 35(11)). Dans ce cas, le processus AIPD doit alors être refait, dans son intégralité ou en partie seulement.

Les facteurs déterminant le changement du niveau de risque varient d'une modification d'une opération de traitement de données au contexte de son déploiement jusqu'au changement d'un élément de la loi de la protection des données à caractère personnel en passant par la pression publique.

EXTRA Indépendamment du changement du niveau de risque, le responsable du traitement peut également décider de revoir le processus AIPD de manière régulière, p.ex. tous les 6 mois, tous les ans, etc.

	Critère		*Changement ?*	*Explication*
Description contextuelle	**Nature** *(quels types d'opérations de traitement ? P.ex. collecte, stockage, effacement, etc.)*		☐	
	Portée	Échelle *(combien ? en quelles quantités ? jusqu'à quel niveau ?)*	☐	
		Période *(quand ? pour combien de temps ?)*	☐	
	Contexte *(dans quelles conditions ?)*	Interne *(par rapport au responsable du traitement)*	☐	
		Externe *(par rapport aux particuliers, aux groupes, à la société, etc.)*	☐	
	Finalité des opérations de traitement, y compris, le cas échéant, l'intérêt légitime *(pourquoi ?)*		☐	

	EXTRA **Avantages** des opérations de traitement	pour les particuliers, y compris les personnes concernées	☐	
		pour le responsable du traitement	☐	
		pour la société dans son ensemble	☐	
	EXTRA **Inconvénients** des opérations de traitement	pour les particuliers, y compris les personnes concernées	☐	
		pour le responsable du traitement	☐	
		pour la société dans son ensemble	☐	
Description technique	Catégories des données à caractère personnel *(quoi ?)* ▪ *catégories particulières de données à caractère personnel* ▪ *données à caractère personnel de personnes vulnérables (p.ex. les enfants)* ▪ *données de nature très personnelle*		☐	
	Moyens du traitement (infrastructure) *(par quels moyens ?)*		☐	
	Flux de données envisagés *(d'où à où ? de qui à qui ?)*		☐	
	Sécurité des données *(comment sont-elles sécurisées)*		☐	
	Domaines de compétences/marché *(où ?)*		☐	
	Acteurs dans la « chaîne d'approvisionnement » *(qui ?)*		☐	
	[Autres, veuillez préciser]		☐	

RECOMMANDATION GÉNÉRALE

Que faire du processus d'analyse ?		*Quand ?*	*Décision du responsable du traitement et justification de sa décision*
☐ réviser	☐ entièrement	*[Veuillez préciser]*	
	☐ en partie *[Veuillez préciser]*	*[Veuillez préciser]*	
☐ ne pas réviser	*[Veuillez préciser pourquoi]*		

COMMENTAIRES

[Explication]

ÉTAPES CONTINUELLES DE LA PHASE III

ÉTAPE A IMPLICATION DES PARTIES PRENANTES

Partie(s) prenante(s) identifiée(s)		*Quelles sont les informations communiquées aux parties prenantes ?*	*Quel retour les parties prenantes ont-elles donné (p.ex. une opinion) ?*	*Comment ce retour a-t-il été intégré ? Pourquoi a-t-il été rejeté ?*
interne	Sous-traitant(s)			
	Délégué(s) à la protection des données (DPD)			
	Destinataire(s) (Article 4(9))			
	Représentant(s) (Article 27)			
	Responsable de la sécurité des systèmes d'information			
	Service juridique			
	Employés, syndicats, contractants, etc.			
	[Autres, veuillez préciser]			
externe	Personne(s) concernée(s)			
	Représentant(s) de la (des) personne(s) concernée(s)			
	Particuliers autres que les personnes concernées			
	Représentant(s) de particuliers autres que les personnes concernées			
	Tiers (Article 4(10)) – secteur public			
	Tiers (Article 4(10)) – secteur privé			
	Experts			
	Autorités de protection des données (APD)			

[Autres, veuillez préciser]			

Absence d'implication des parties prenantes dans la présente phase

[Si les parties prenantes ne sont pas impliquées dans la présente phase du processus AIPD, veuillez expliquer pourquoi il en est ainsi.]

ÉTAPE B* CONTRÔLE DE QUALITÉ

Organe de contrôle de qualité.	*Quel retour a été reçu ?*	*Comment ce retour a-t-il été implémenté ?* *Pourquoi a-t-il été rejeté ?*
Délégué à la protection des données (DPD)		
Autorités de protection des données (APD)		
[Autres, veuillez préciser]		

Absence de contrôle de qualité dans la présente phase

[Si la qualité n'a pas été contrôlée dans la présente phase du processus AIPD, veuillez expliquer pourquoi il en est ainsi]

COMMENTAIRES

[Explication]

DERNIÈRE PAGE

MENTIONS

Nom	*Rôle*	*Observations*	*Signature*	*Date*
	Évaluateur(s)			
	Délégué à la protection des données			
	Responsable(s) du traitement			
	[Autres, veuillez préciser]			

ÉTAPE C* DOCUMENTATION

Objectif

Le but de cette étape continuelle consiste à conserver des documents intelligibles sous forme écrite ou sous toute autre forme permanente (analogue of numérique) de toutes les activités entreprises au cours d'un processus d'analyse déterminé, tout en respectant les éléments qui doivent légitimement rester secrets.

Mise en œuvre

La documentation consiste du présent rapport et de toutes les annexes énumérées ci-dessous, tant les versions préliminaires que définitives. Les évaluateurs dressent également une liste de toutes les activités entreprises au cours d'un processus d'analyse déterminé, p.ex. les versions préliminaires du présent rapport ou les interactions avec les personnes concernées, les APDs, etc.

Il pourrait y avoir un registre (national) des processus AIPD réalisés auquel les évaluateurs doivent ou sont invités à soumettre leur rapport sur le processus AIPD.

Il est également recommandé de rendre le rapport ou des parties du rapport, ainsi que les annexes, accessibles au public (p.ex. à travers le site web du responsable du traitement), tout en respectant les éléments qui doivent légitimement rester secrets. Après révision du processus d'analyse, une nouvelle version du rapport sera également rendue accessible au public, en faisant référence à la version précédente.

ACTIVITÉS ENTREPRISES AU COURS DU PROCESSUS AIPD

Date	*Acteur*	*Activité*	*Description*	*Commentaires*
[Veuillez préciser]				

ANNEXES

	Annexe	*Niveau de confidence*	*Annexé ?*	*Commentaires*
Étape 1 Étape 4	Registre des activités de traitement		☐	
Étape 2	Codes de conduite approuvés		☐	

	Certifications		☐	
	Règles d'entreprise contraignantes (REC)		☐	
	Clauses contractuelles types (CCT)		☐	
	Politiques de protection des données		☐	
	Codes de conduite professionnelle		☐	
	Contrat(s) d'échange de données	confidentiel	☐	
Étape 3	Une copie du contrat de service (dans le cas où le AIPD est externalisé).		☐	
	Une liste des parties prenantes à des fins de consultation comprenant leurs coordonnées	confidentiel	☐	
	Plan de consultation des parties prenantes		☐	
Étape 7	Demande de consultation préalable auprès d'une APD		☐	
	Réponse d'une autorité de contrôle		☐	
Étape A	Exposé(s) technique(s) pour consultation des parties prenantes		☐	
	Consultation des parties prenantes (rapports)		☐	
	Opinion du DPD (rapport)		☐	
	[Rapports d'autres techniques d'évaluation ; veuillez préciser]		☐	
	[Autres, veuillez préciser]		☐	

COMMENTAIRES

[Explication]

2 REMARQUES FINALES

Dans la présente Note de Politique, d.pia.lab propose un modèle pour réaliser un processus AIPD au sein de l'UE/EEE, lequel est basé sur une interprétation des obligations légales pertinentes du RGPD et qui reflète les meilleures pratiques pour la réalisation d'une analyse d'impact. Aucun élément du modèle proposé n'est cependant définitif. Il doit encore être testé et ensuite révisé en fonction des expériences acquises lors de son utilisation. Pour cette raison, d.pia.lab désire recevoir des commentaires sur le modèle proposé, notamment pour intégrer ceux-ci dans ses révisions futures.

En parallèle, l'« architecture » de l'analyse d'impact ne se limite pas au cadre, à la méthode et au modèle. D'autres éléments, principalement de nature technique, tels qu'une liste des aspects pouvant présenter des risques pour les droits et les libertés de particuliers ainsi qu'une liste de potentielles contremesures permettant d'y remédier (des « bases de connaissances ») doivent être développés, testés et révisés en fonction des expériences acquises lors de leurs utilisation. d.pia.lab traitera ses éléments dans ses travaux futurs.

SÉLECTION DE SOURCES PERTINENTES

Margaret Hagan (n.d.) *Law by Design*, https://www.lawbydesign.co.

Kloza, Dariusz, Niels van Dijk, Raphaël Gellert, István Böröcz, Alessia Tanas, Eugenio Mantovani etPaul Quinn (2017) "Analyse d'impact relative à la protection des données dans l'Union européenne : une protection des personnes plus solide en complétant le nouveau cadre juridique", d.pia.lab Note de Politique No. 1/2017, VUB: Bruxelles. https://cris.vub.be/files/37820556/dpialab_pb2017_1_final_FR.pdf.

Kloza, Dariusz, Niels van Dijk, Simone Casiraghi, Sergi Vazquez Maymir, Sara Roda, Alessia Tanas et Ioulia Konstantinou (2019) "Vers une méthode pour réaliser l'analyse d'impact relative à la protection des données: Comprendre et interpréter les obligations du RGPD", *d.pia.lab* Note Politique No. 1/2019, VUB: Bruxelles. https://cris.vub.be/files/48762435/dpialab_pb2019_1_final_FR.pdf.

Möller, Kai (2012) "Proportionality: Challenging the Critics", *International Journal of Constitutional Law*, 10(3), 709–731. doi: 10.1093/icon/mos024.

Peers, Steve, and Sacha Prechal (2015) "Article 52: Scope and Interpretation of Rights and Principles", in: Steve Peers, Tamara Hervey, Jeff Kenner and Angela Ward (eds.) *The EU Charter of Fundamental Rights: A Commentary*, 1455–1522, Hart Publishing: London. doi: 10.5040/9781849468350.ch-056.

AUTRES LECTURES : LES PRINCIPAUX CONCEPTS

Barak, Aharon (2012) *Proportionnalité: Constitutional Rights and their Limitations*, Cambridge University Press: Cambridge. doi: 10.1017/CBO9781139035293.

Brkan, Maja (2019) "The Essence of the Fundamental Rights to Privacy and Data Protection: Finding the Way Through the Maze of the CJEU's Constitutional Reasoning", *German Law Journal*, 20(6), 864–883. doi: 10.1017/glj.2019.66.

AUTRES LECTURES : GUIDES PRATIQUES

Agencia Española de Protección de Datos [AEPD] (2018) *Guía práctica para las Evaluaciones de Impacto en la Protección de los datos sujetas al RGPD*, Madrid. https://www.aepd.es/sites/default/files/2019-09/guia-evaluaciones-de-impacto-rgpd.pdf.

Groupe de travail « Article 29 » sur la protection des données (2017) *Lignes directrices concernant l'analyse d'impact relative à la protection des données (AIPD) et la manière de déterminer si le traitement est «susceptible d'engendrer un risque élevé» aux fins du règlement (UE)2016/679*, WP248 rev. 01, Bruxelles. https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236.

Commission Nationale de l'Informatique et des Libertés [CNIL] (2018) *Analyse d'impact relative à la protection des données (AIPD) 3 : les bases de connaissances*, Paris. https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-3-fr-basesdeconnaissances.pdf.

European Data Protection Supervisor [EDPS] (2018) *Accountability on the ground. Phase II : Data Protection Impact Assessments & Prior Consultation*, Brussels. https://edps.europa.eu/sites/edp/files/publication/18-02-06_accountability_on_the_ground_part_2_en.pdf.

EDPS (2017) *Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit*, Brussels. https://edps.europa.eu/sites/edp/files/publication/17-04-11_necessity_toolkit_en_0.pdf.

EDPS (2019) *Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data*, Brussels. https://edps.europa.eu/sites/edp/files/publication/19-12-19_edps_proportionality_guidelines2_en.pdf.

International Association of Privacy Professionals [IAPP] (2020) *2020 Privacy Tech Vendor Report*, Portsmouth, NH. https://iapp.org/resources/article/privacy-tech-vendor-report.

International Organization for Standardization [ISO] (2018) *Risk management – Guidelines*, ISO 31000:2018, Geneva. https://www.iso.org/iso-31000-risk-management.html.

ISO (2018) *Renseignements technology – Sécurité techniques – Renseignements sécurité risque management*, ISO 27005:2018, Geneva. https://www.iso.org/standard/75281.html.

ISO (2019) *Sécurité and resilience – Business continuité management sécurité – Requirements*, ISO 22301:2019, Geneva. https://www.iso.org/standard/75106.html.

Mays, Claire (2004) *Stakeholder Involvement Techniques. Short Guide and Annotated Bibliography*, Organisation for Economic Co-operation and Development (OECD), Paris. http://www.oecd-nea.org/rwm/reports/2004/nea5418-stakeholder.pdf.

Sammut-Bonnici, Tanya, and David Galea (2015) "SWOT Analysis", in: Cary L. Cooper (ed.) *Wiley Encyclopedia of Management*, 1-8, John Wiley & Sons: Chichester. doi: 10.1002/9781118785317.weom120103.

A PROPOS DE D.PIA.LAB

Le **Brussels Laboratory for Data Protection & Privacy Impact Assessments**, ou **d.pia.lab**, relie la recherche fondamentale, méthodologique et appliquée, donne des formations et prodigue des conseils stratégiques et politiques sur les analyses d'impact relevant des domaines de l'innovation et du développement technologique. Quoique les aspects juridiques de la protection des données personnelles et de la vie privée constituent les axes prioritaires de notre Laboratoire, nos activités englobent également d'autres disciplines telles que l'éthique et la philosophie ainsi que les études de surveillance et les études des sciences, des technologies & de la société (STS) Créé en novembre 2015, le Laboratoire fait partie intégrante de et s'appuie sur l'expérience du Research Group on Law, Science, Technology & Society (LSTS) établi à la Vrije Universiteit Brussel (VUB), Belgique.

Le Laboratoire a développé sa base de connaissance en matière d'analyses d'impact à partir de plusieurs projets de recherche finalisés et en cours tels que PERSONA, HR-RECYCLER and SYSTEM (cofinancé par l'UE). Les opinions exprimées dans la présente Note Politique ne reflètent pas nécessairement celles des bailleurs de fonds.

Nous tenons à remercier les personnes suivants (en order alphabétique), Jonas Breuer, Athena Christofi, Roger Clarke, Katerina Demetzou, Pierre Dewitte, Laura Drechsler, Rossana Ducato, Anna Johnston, Kristoffer Lidén, Gianclaudio Malgieri, Rotem Medzini, Anna Mościbroda, Laurens Naudts, Juraj Sajfert, Mistale Taylor et Heidi Waem pour leurs précieux commentaires sur une version précédente de la présente Note de Politique. Traduction en français par Sleutelwoord | Mot-clé bvba (novembre 2020).

dpialab.org | **dpialab@vub.ac.be**