Recommandation n° 01/2018 du 28 février 2018

Objet : Recommandation d'initiative concernant l'analyse d'impact relative à la protection des données et la consultation préalable (CO-AR-2018-001)

La Commission de la protection de la vie privée (ci-après "la Commission") ;

Vu la loi du 8 décembre 1992 *relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel* (ci-après "la LVP"), en particulier l'article 30 ;

Vu le Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 *relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE* (règlement général sur la protection des données, ci-après RGPD), en particulier les articles 35 et 36 ;

Vu les articles 26 et 27 de la Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 *relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données et abrogeant la décision-cadre 2008/977/JAI du Conseil* ;

Vu le rapport de Willem Debeuckelaere ;

Émet, le 28 février 2018, la recommandation suivante :

1. Introduction 4

2. Pourquoi une AIPD ?..... 6

3. Quand une AIPD est-elle requise ?..... 7

A) Lorsque le traitement est "susceptible d'engendrer un risque élevé" pour les droits et libertés des personnes physiques 7

B) Les traitements mentionnés à l'article 35(3) du RGPD 12

C) Les listes de l'autorité de contrôle 14

4. À quel moment doit-on réaliser une AIPD ? 15

5. Quels sont les éléments essentiels d'une AIPD ? 16

A) Aperçu 16

B) Description des opérations de traitement envisagées et des finalités du traitement 16

C) Contrôle de la proportionnalité.....17

D) Évaluation des risques.....19

E) Mesures visées 24

6. Quand une consultation préalable est-elle requise ?.....25

7. Qui assure quel rôle lors de l'exécution d'une AIPD ? 27

A) Le(s) responsable(s) du traitement 27

B) Le sous-traitant 29

C) Le délégué à la protection des données.....30

D) Les personnes concernées ou leurs représentants.....31

E) L'autorité de contrôle 32

F) Le grand public.....33

8. Dispositions particulières.....33

A) Traitement en vertu d'une obligation légale ou de l'intérêt public 33

B) Opérations de traitement similaires ou conjointes 34

C) Codes de conduite 35

D) Gestion et contrôle.....35

E) Quid des traitements déjà existants ?.....37

F) Amende possible en cas de non-respect 38

9. Annexe 1 : Caractéristiques minimales d'une bonne gestion des risques 39

10. Annexe 2 : Projet de liste des types d'opérations de traitement pour lesquelles une AIPD est requise (art. 35(4) du RGPD) 42

11. Annexe 3 : Projet de liste des types d'opérations de traitement pour lesquelles aucune AIPD n'est requise (art. 35(5) du RGPD) 45

1. Introduction

1. Le Règlement général sur la protection des données (RGPD) prévoit plusieurs nouvelles obligations pour les responsables du traitement[1]. Une des nouvelles obligations figurant dans le RGPD concerne l'obligation de réaliser - dans certaines circonstances - une "analyse d'impact relative à la protection des données", en abrégé "AIPD".

2. Une AIPD est un **processus** dont l'objet est de **décrire** le traitement de données à caractère personnel, d'en **évaluer la nécessité ainsi que la proportionnalité** et d'aider à **gérer** les **risques** pour les droits et libertés des personnes physiques qui y sont liés en les évaluant et en déterminant les mesures nécessaires pour y faire face[2].

3. La Directive Police et Justice (Directive 2016/680) prévoit également une obligation de réaliser une AIPD dans certaines circonstances[3]. Les lignes directrices reprises dans la présente recommandation, qui s'inspirent des dispositions du RGPD, s'appliquent *mutatis mutandis* pour l'interprétation des dispositions pertinentes de la Directive 2016/680.

4. Le but de la présente recommandation est de fournir des explications plus détaillées concernant :

(1) les circonstances dans lesquelles une AIPD est obligatoire (section 3) ;

(2) les éléments essentiels d'une AIPD (section 5) ;

(3) les circonstances dans lesquelles une consultation préalable est obligatoire (section 6) ;

(4) les acteurs qui doivent être impliqués dans une AIPD (section 7) ; et

(5) plusieurs dispositions particulières (section 8).

5. Un précédent projet de recommandation a été soumis à une consultation publique du 20 décembre 2016 au 28 février 2017[4]. La présente recommandation tient compte des remarques et suggestions qui ont été formulées par des entreprises, des fédérations sectorielles et des

---

[1] Là où la version néerlandaise de la Directive 95/46/CE renvoyait au "voor de verwerking verantwoordelijke", le RGPD renvoie au "verwerkingsverantwoordelijke". NdT : cette différence ne se reflète pas dans la version française du texte.

[2] Groupe de protection des données Article 29, Lignes directrices concernant l'analyse d'impact relative à la protection des données (AIPD) et la manière de déterminer si le traitement est "susceptible d'engendrer un risque élevé" aux fins du règlement (UE) 2016/679, WP 248 rev.01, 4 octobre 2017, p. 4. (ci-après : "Groupe 29, Lignes directrices AIPD"). La notion d' "analyse d'impact relative à la protection des données" n'est pas définie en tant que telle dans le RGPD mais est expliquée comme suit dans le considérant (84) du RGPD : "*Afin de mieux garantir le respect du présent règlement lorsque les opérations de traitement sont susceptibles d'engendrer un risque élevé pour les droits et libertés des personnes physiques, le responsable du traitement ou le sous-traitant devrait assumer la responsabilité d'effectuer une analyse d'impact relative à la protection des données pour évaluer, en particulier, l'origine, la nature, la particularité et la gravité de ce risque.*" En ce qui concerne la notion de "risque", voir ci-après au point 16.

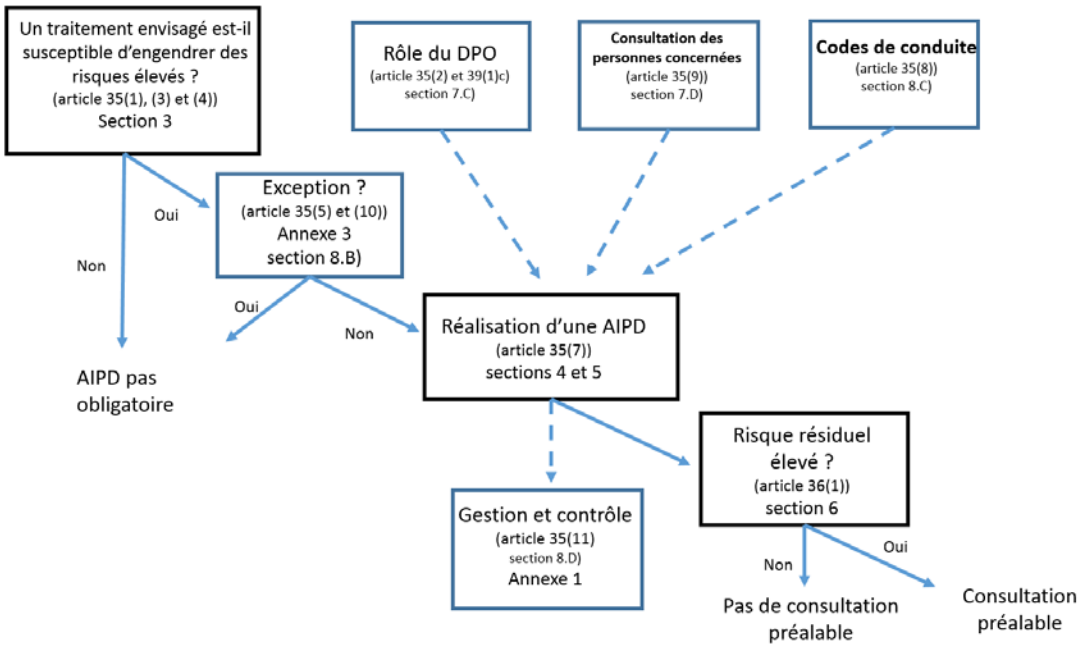
[3] Voir les articles 27-28 de la Directive 2016/680.

[4] https://www.privacycommission.be/fr/consultation-publique-sur-la-recommandation-concernant-lanalyse-dimpact-relative-a-la-protection.

universitaires, ainsi que de la version finale des lignes directrices du Groupe de protection des données Article 29 promulguées en octobre 2017.

6. La présente recommandation ne comporte aucun modèle établi, ni de vade-mecum pour la réalisation d'une AIPD. Bien qu'il existe plusieurs modèles et vade-mecum[5], la Commission encourage les fédérations sectorielles à élaborer des codes de conduite adaptés aux traitements de données au sein de leur secteur et qui sont adaptés en particulier aux besoins des petites, moyennes et micro-entreprises[6]. Il n'est toutefois pas exclu qu'à l'avenir, la Commission mette à disposition un formulaire et/ou un vade-mecum complémentaire qui pourrait servir de point de départ à la réalisation d'une AIPD ou dans le cadre d'une consultation préalable.

7. Pour guider le lecteur au fil de cette recommandation et permettre un accès rapide aux parties pertinentes, le schéma suivant peut s'avérer utile :



[5] Voir l'Annexe 1 du Groupe 29, Lignes directrices AIPD, p. 26. Voir également ci-après par exemple Banque Carrefour de la Sécurité Sociale, "RGPD Risk Register", disponible à l'adresse https://www.ksz-bcss.fgov.be/sites/default/files/assets/securite_et_vie_privee/avg_risk_register_fr.xlsm et Rijksoverheid, Model gegevensbeschermings.effectbeoordeling rijksdienst (PIA), Septembre 2017, disponible à l'adresse https://www.rijksoverheid.nl/documenten/rapporten/2017/09/29/model-gegevensbeschermingseffectbeoordeling-rijksdienst-pia (ci-après : "Rijksoverheid, Model PIA").

[6] Voir également le bloc thématique "Codes de conduite sous le nouveau règlement", https://www.privacycommission.be/fr/codes-de-conduite-sous-le-nouveau-reglement.

2. Pourquoi une AIPD ?

8. L'obligation de procéder - dans certaines circonstances - à une AIPD doit être examinée à la lumière de deux principes centraux du RGPD, à savoir le principe de la responsabilité et le principe de l'approche fondée sur les risques.

9. Le principe de la responsabilité (ce qu'on appelle l' "***accountability***") implique que le responsable du traitement n'est pas uniquement tenu de respecter les principes et obligations du RGPD mais qu'il doit également pouvoir démontrer qu'il les respecte[7]. L'AIPD constitue un instrument important à cet égard, étant donné qu'elle peut contribuer aussi bien au respect des principes et obligations du RGPD qu'à la démonstration de ce respect.

10. Le principe de la responsabilité va de pair avec une approche fondée sur les risques (ce qu'on appelle une ***"risk-based approach***")[8]. Le RGPD requiert que les responsables du traitement prennent des mesures adéquates afin de garantir le respect du RGPD, compte tenu notamment "*des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques*"[9]. L'obligation pour les responsables du traitement d'effectuer une AIPD dans certaines situations doit être comprise dans le contexte de leur obligation générale de gérer de manière appropriée les risques que présente le traitement de données personnelles[10]. Le simple fait que les conditions déclenchant l'obligation d'effectuer une AIPD ne soient pas remplies ne restreint toutefois pas l'exigence générale faite aux responsables du traitement de mettre en oeuvre des mesures pour gérer de manière appropriée les risques pour les droits et libertés des personnes concernées[11].

11. L'approche fondée sur les risques du RGPD a pour but de promouvoir une "**approche évolutive et proportionnelle**"[12] sans remettre en question les principes de protection des données ou les droits des personnes concernées[13]. Cela signifie qu'il faudra prendre davantage de mesures de protection pour des traitements présentant un risque élevé que pour des traitements à risque faible.

---

[7] L'article 5(2) du RGPD dispose que : "*Le responsable du traitement est responsable du respect du paragraphe 1 et est en mesure de démontrer que celui-ci est respecté (responsabilité)*".

[8] Voir l'Article 29 Data Protection Working Party, "Statement on the role of a risk-based approach in data protection legal frameworks", (librement traduit : "Déclaration du Groupe 29 du 30 mai 2014 sur le rôle d'une approche fondée sur les risques dans des cadres juridiques de protection des données"), WP 218 du 30 mai 2014.

[9] Article 24(1) du RGPD.

[10] Groupe 29, Lignes directrices AIPD, p. 7.

[11] Dans la pratique, cela signifie donc que les responsables du traitement doivent évaluer en permanence les risques engendrés par leurs activités de traitement afin de pouvoir établir qu'un type de traitement "est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques". Groupe 29, Lignes directrices AIPD, p. 7.

[12] En anglais : "*a scalable and proportionate approach to compliance*". (Article 29 Data Protection Working Party, "Statement on the role of a risk-based approach in data protection legal frameworks", p. 2).

[13] L'approche fondée sur les risques ne dispense pas le responsable du traitement de son obligation de respecter les principes et obligations du RGPD. Ainsi, les principes en matière de qualité des données et les droits des personnes concernées doivent toujours être respectés, quels que soient les risques qu'un traitement déterminé engendre. (*Id.*)

12. L'obligation de procéder à une AIPD a été élaborée dans le contexte de la Directive 95/46/CE qui prévoyait une obligation générale de notifier chaque traitement de données à caractère personnel aux autorités de contrôle. Cette obligation générait une charge administrative et financière, sans nécessairement améliorer le niveau de protection pour les données à caractère personnel[14]. Le nouveau système met dès lors l'accent sur l'obligation du responsable du traitement de réaliser une AIPD préalable pour les traitements "susceptibles d'engendrer un risque élevé" et sur les mesures pouvant être prises afin de réduire ces risques.

13. Enfin, la réalisation d'une AIPD peut aider le responsable du traitement à respecter l'obligation de protection des données dès la conception (ce qu'on appelle en anglais la "***data protection by design***"). L'article 25(1) du RGPD oblige le responsable du traitement à prendre les mesures techniques et organisationnelles appropriées, tant au moment de la détermination des moyens du traitement qu'au moment du traitement lui-même. Étant donné qu'une AIPD sert justement, avant le traitement, à identifier les mesures pour faire face aux risques pour les droits et libertés des personnes physiques, l'AIPD peut jouer à cet égard un rôle important d'appui et/ou de guide.

3. Quand une AIPD est-elle requise ?

14. Le RGPD ne requiert pas que le responsable du traitement procède à une AIPD pour chaque traitement de données à caractère personnel. En règle générale, une AIPD n'est requise que lorsque le traitement de données, compte tenu de sa nature, de sa portée, de son contexte et de ses finalités, *est susceptible d'engendrer un risque élevé* pour les droits et libertés des personnes physiques[15]. En outre, l'article 35(3) du RGPD énumère un certain nombre de cas où une AIPD est toujours requise (pour lesquels le législateur européen a donc établi qu'il s'agissait de traitements qui étaient par nature "susceptibles d'engendrer un risque élevé"). Enfin, l'article 35(4) et l'article 35(5) du RGPD prévoient que toute autorité de contrôle nationale établit des listes des types d'opérations de traitement pour lesquelles une AIPD est requise ou non.

A) Lorsque le traitement est "susceptible d'engendrer un risque élevé" pour les droits et libertés des personnes physiques

15. L'article 35(1) du RGPD dispose que :

"*Lorsqu'un type de traitement, en particulier par le recours à de nouvelles technologies, et compte tenu de la nature, de la portée, du contexte et des finalités du traitement, est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, le responsable du*

[14] Considérant (89) du RGPD.

[15] Article 35(1) du RGPD.

traitement effectue, avant le traitement, une analyse de l'impact des opérations de traitement envisagées sur la protection des données à caractère personnel."

- *Qu'est-ce qu'un "risque" ?*

16. Un "risque" est un scénario qui décrit un événement et ses effets, estimés en termes de gravité et de probabilité[16]. Autrement dit, un risque est la possibilité ("**probabilité**") qu'un événement ou une menace déterminé(e) se produise, entraînant un **impact** ("gravité") déterminé[17]. L'article 35(1) du RGPD renvoie à une catégorie particulière de risques, à savoir les *risques pour les droits et libertés des personnes physiques*[18]*.* Dans le cadre d'une AIPD, un "risque" est donc une possibilité que survienne une conséquence négative pour les droits et libertés des personnes physiques, résultant d'un traitement de données à caractère personnel[19]. La manière d'interpréter cette notion en pratique est expliquée ci-après dans la section 5[20].

- *Qu'est-ce qu'un "risque élevé" ?*

17. La notion de "risque élevé" n'est pas définie plus en détail dans le RGPD. La Commission est consciente du fait que des organisations différentes utilisent des échelles et des méthodes différentes lorsqu'elles procèdent à une évaluation des risques. Il est dès lors possible que l'interprétation de ces valeurs diffère, selon l'échelle de risque et la méthode utilisées. La notion de "risque élevé" au sens du RGPD ne correspond toutefois pas nécessairement à la notion de "risque élevé" telle qu'on la retrouve dans d'autres modèles de gestion des risques.

18. La Commission estime que la notion de "risque élevé" renvoie aux traitements de données qui sont ou pourront être **susceptibles** d'avoir des **incidences négatives sensibles** pour les libertés et droits fondamentaux des personnes physiques. L'expression "susceptible de" ne signifie pas qu'il existe une lointaine possibilité d'incidence sensible. L'incidence sensible doit être plus probable qu'improbable. En revanche, cela signifie également qu'il n'est pas nécessaire que les personnes soient réellement affectées : la probabilité qu'elles soient sensiblement affectées suffit pour répondre à ce

[16] Groupe 29, Lignes directrices AIPD, p. 7.

[17] Voir également ISO, "Risk management – Vocabulary", ISO Guide 73:2009 ("*un risque est souvent exprimé en termes de combinaison des conséquences d'un événement (incluant des changements de circonstances) et de sa vraisemblance*").

[18] Étant donné qu'une AIPD est un instrument de gestion des risques pour les droits des personnes concernées, la perspective de la personne concernée est centrale. Cette situation est différente de la gestion de risques dans d'autres domaines (comme par exemple la sécurité de l'information), qui est généralement axée sur les intérêts et les finalités de l'organisation elle-même. (Voir aussi Groupe 29, Lignes directrices AIPD, p. 21.)

[19] Rijksoverheid, Model PIA, p. 35.

[20] Voir ci-après, les points 45 e.s.

critère[21]. Une "conséquence négative sensible" signifie que, dans le cas où le risque se produirait, la personne concernée serait sensiblement affectée dans l'exercice ou la jouissance de ses libertés et droits fondamentaux[22].

- *Quand est-il question d'un risque élevé probable ?*

19. Pour déterminer s'il est ou non probable qu'un traitement envisagé puisse donner lieu à un risque élevé, les lignes directrices élaborées par le Groupe 29 sont particulièrement importantes[23]. Le Groupe 29 a identifié **neuf critères** que les responsables du traitement doivent prendre en considération dans leur analyse déterminant si un traitement envisagé est ou non *susceptible d'engendrer un risque élevé* pour les droits et libertés des personnes physiques. Ces critères sont les suivants :

1. Évaluation ou notation, y compris les activités de profilage et de prédiction, portant notamment sur des "aspects concernant le rendement au travail de la personne concernée, sa situation économique, sa santé, ses préférences ou centres d'intérêt personnels, sa fiabilité ou son comportement, ou sa localisation et ses déplacements"[24].
2. Prise de décision automatisée avec effet juridique ou effet similaire significatif : ce critère comprend des traitements axés sur la prise de décisions relatives aux personnes concernées produisant des effets juridiques à l'égard d'une personne physique ou l'affectant de manière significative de façon similaire[25].
3. Surveillance systématique : ce critère comporte des traitements utilisés pour observer, surveiller ou contrôler les personnes concernées, y compris la collecte de données via des réseaux et par la surveillance systématique d'une zone accessible au public[26]. Il s'agit d'un critère étant donné que la collecte des données à caractère personnel est susceptible d'intervenir dans des circonstances telles que les personnes concernées ne savent pas qui collecte leurs données et de quelle façon

[21] Groupe de protection des données Article 29, Lignes directrices concernant la désignation d'une autorité de contrôle chef de file d'un responsable du traitement ou d'un sous-traitant, WP 244 rev.01, 5 avril 2017, p. 4. Voir aussi ci-après les points 45 e.s., pour quelques exemples spécifiques.

[22] Pour l'interprétation de la notion "affecte sensiblement", voir également le Groupe de protection des données Article 29, Lignes directrices concernant la désignation d'une autorité de contrôle chef de file d'un responsable du traitement ou d'un sous-traitant, WP 244 rev.01, 5 avril 2017, p. 4 (explication des notions " sont sensiblement affectées (…) ou sont susceptibles de l'être" au sens de l'article 4(23) du RGPD).

[23] Groupe 29, Lignes directrices AIPD, p. 10-13.

[24] Voir également les considérants (71), (75) et (91) du RGPD. À titre d'exemples, prenons le cas d'un établissement financier passant ses clients au crible d'une base de données de cote de crédit ou d'une base de données dédiée à la lutte contre le blanchiment de capitaux et le financement du terrorisme (LBC/FT) ou "antifraude", celui d'une société de biotechnologie proposant des tests génétiques directement aux consommateurs afin d'évaluer et de prédire les risques de maladie/de problèmes de santé, ou encore celui d'une entreprise analysant les usages ou la navigation sur son site Web pour créer des profils comportementaux ou marketing.

[25] Voir également l'article 35(3)a du RGPD. Ce critère est présent lorsque le traitement peut par exemple entraîner l'exclusion ou une discrimination de personnes physiques. Un traitement n'ayant que peu ou pas d'effet sur les personnes physiques ne répond pas à ce critère particulier. Des explications complémentaires concernant ces notions sont fournies dans les lignes directrices du Groupe 29 relatives au profilage.

[26] Voir également l'article 35(3)c du RGPD. En ce qui concerne l'interprétation de la notion de "systématique", voir ci-après le point 24

elles seront utilisées. En outre, il peut être impossible pour les personnes de se soustraire à un tel traitement dans l'espace public (ou accessible au public) considéré[27].

4. Données sensibles ou données à caractère hautement personnel : ce critère comporte les catégories particulières de données à caractère personnel visées à l'article 9 (informations concernant les opinions politiques des personnes, par exemple) ainsi que des données à caractère personnel relatives aux condamnations pénales ou aux infractions visées à l'article 10[28]. Il comporte également les données à caractère personnel qui sont considérées de manière générale comme sensibles dans la mesure où elles sont liées à des activités domestiques et privées (communications électroniques dont la confidentialité doit être protégée, par exemple), dans la mesure où elles ont un impact sur l'exercice d'un droit fondamental (données de localisation dont la collecte peut influencer la liberté de mouvement, par exemple) ou dans la mesure où leur divulgation aurait clairement des incidences graves dans la vie quotidienne de la personne concernée (données financières susceptibles d'être utilisées pour des paiements frauduleux, par exemple)[29].

5. Traitement de données à caractère personnel à grande échelle, compte tenu :
   - du nombre de personnes concernées (soit en valeur absolue, soit en proportion de la population considérée) ;
   - du volume de données et/ou de l'éventail des différents éléments de données traitées ;
   - de la durée ou de la permanence de l'activité de traitement de données ;
   - de l'étendue géographique de l'activité de traitement[30].

6. Croisement ou combinaison d'ensembles de données, par exemple issus de deux opérations de traitement de données, ou plus, effectuées à des fins différentes et/ou par différents responsables du traitement, d'une manière qui outrepasserait les attentes raisonnables de la personne concernée[31].

---

[27] Exemples d'activités pouvant constituer un suivi régulier et systématique des personnes concernées : exploitation d'un réseau de télécommunications; fourniture de services de télécommunications; reciblage par courrier électronique; activités de marketing fondées sur les données; profilage et notation à des fins d'évaluation des risques (par exemple, aux fins de l'évaluation du risque de crédit, de l'établissement des primes d'assurance, de la prévention de la fraude ou de la détection du blanchiment d'argent) ; géolocalisation, par exemple, par des applications mobiles; programmes de fidélité; publicité comportementale; surveillance des données sur le bien-être, la santé et la condition physique au moyen de dispositifs portables; systèmes de télévision en circuit fermé; dispositifs connectés tels que les voitures et compteurs intelligents, la domotique, etc. (Groupe de protection des données Article 29, Lignes directrices concernant les délégués à la protection des données (DPD), WP 243 rev.01, 5 avril 2017, p. 11) (ci-après: "Groupe 29, Lignes directrices concernant les délégués à la protection des données").

[28] Voir également le considérant (45) du RGPD. À titre d'exemple, citons les dossiers médicaux que peut conserver un hôpital général ou encore les informations sur des auteurs d'infractions que peut détenir un enquêteur privé.

[29] Ce critère peut également inclure les données telles que les documents personnels, les courriers électroniques, les agendas, les notes des liseuses équipées de fonctions de prise de notes ainsi que les informations à caractère très personnel contenues dans les applications de "life-logging". Lors de l'évaluation de ce critère, il peut être pertinent de savoir si les données ont déjà été rendues publiques par la personne concernée ou par des tiers. Le fait que des données à caractère personnel soient publiques peut être considéré comme un facteur dans l'évaluation de savoir si l'on s'attend à ce que les données seront utilisées ultérieurement à certaines fins.

[30] Voir également les considérants (75) et (91) du RGPD. Voir aussi Groupe 29, Lignes directrices concernant les délégués à la protection des données, p. 9.

[31] Voir aussi ci-après l'explication reprise dans l'avis WP29 relatif à la limitation de la finalité (WP 203), p. 24.

7. Données concernant des personnes vulnérables, comme par exemple les enfants, les travailleurs, les personnes souffrant de maladie mentale, les demandeurs d'asile, les personnes âgées, les patients et autres segments les plus vulnérables de la population nécessitant une protection particulière[32]. Le traitement de ce type de données est un critère en raison du déséquilibre des pouvoirs accru qui existe entre les personnes concernées et le responsable du traitement, ce qui signifie que les premières peuvent se trouver dans l'incapacité de consentir, ou de s'opposer aisément au traitement de leurs données ou d'exercer leurs droits.

8. Utilisation ou application innovante de nouvelles solutions technologiques ou organisationnelles, comme l'utilisation combinée de systèmes de reconnaissance des empreintes digitales et de reconnaissance faciale pour améliorer le contrôle des accès physiques, etc. Il s'agit d'un critère parce que l'utilisation de la technologie en question peut impliquer de nouvelles formes de collecte et d'utilisation des données, présentant potentiellement un risque élevé pour les droits et libertés des personnes physiques[33].

9. Lorsque, du fait du traitement lui-même, les personnes concernées ne peuvent pas exercer un droit ou bénéficier d'un service ou d'un contrat[34]. Cela comprend les opérations visant à autoriser, modifier ou refuser l'accès des personnes concernées à un service ou la possibilité de ces personnes de conclure un contrat[35].

20. Dans la plupart des cas, un responsable du traitement peut partir du principe que si un traitement répond à **deux critères**, une analyse d'impact relative à la protection des données doit être réalisée. De manière générale, le Groupe 29 considère que plus le nombre de critères auxquels le traitement répond est élevé, plus il est probable qu'il implique un risque élevé pour les droits et libertés des personnes concernées, et donc qu'il requière une AIPD, quelles que soient les mesures que le responsable du traitement a l'intention de prendre pour limiter les risques[36]. Dans certains cas, un responsable du traitement peut toutefois estimer qu'un traitement qui ne répond qu'à un seul de ces critères requiert une analyse d'impact relative à la protection des données[37].

21. À l'inverse, il est possible qu'un responsable du traitement ne considère pas un traitement qui correspond pourtant aux cas précités comme un traitement "susceptible d'engendrer un risque élevé". Dans de tels cas, le responsable du traitement doit **motiver et documenter** les raisons pour

---

[32] Voir également le considérant (75) du RGPD.

[33] En outre, il est clairement précisé dans le RGPD que l'utilisation d'une nouvelle technologie peut impliquer la nécessité de réaliser une analyse d'impact relative à la protection des données. Voir l'article 35(1) et les considérants (89) et (91) du RGPD. Le fait de déterminer si une technologie doit être considérée ou non comme étant "nouvelle" doit se faire "en conformité avec l'état des connaissances technologiques".

[34] Voir l'article 22 et le considérant (91) du RGPD.

[35] À titre d'exemple, prenons le cas d'une banque passant ses clients au crible d'une base de données de cote de crédit avant d'arrêter ses décisions d'octroi de prêt.

[36] Pour des exemples supplémentaires d'application de ces critères, voir Groupe 29, Lignes directrices AIPD, p. 13-14.

[37] Groupe 29, Lignes directrices AIPD, p. 13.

lesquelles aucune analyse d'impact relative à la protection des données n'a été réalisée et il doit consigner/enregistrer dans cette documentation les avis du délégué à la protection des données[38]. Même si le responsable du traitement en arrive à la conclusion que la réalisation d'une AIPD n'est pas requise, il reste soumis à son obligation générale de gestion adéquate des risques, conformément à l'article 24(1) du RGPD[39].

B) Les traitements mentionnés à l'article 35(3) du RGPD

22. L'article 35(3) du RGPD énumère **trois situations** dans lesquelles une AIPD est toujours requise :

a) en cas d'évaluation *systématique et approfondie d'aspects personnels concernant des personnes physiques* qui est fondée sur un traitement automatisé, y compris le profilage, et sur la base de laquelle sont prises des *décisions* produisant des effets juridiques à l'égard d'une personne physique ou l'affectant de manière significative de façon similaire ;

b) en cas de *traitement à grande échelle de catégories particulières de données à caractère personnel* visées à l'article 9, paragraphe 1, ou de données à caractère personnel relatives à des condamnations pénales et à des infractions visées à l'article 10 ; ou

c) en cas de *surveillance systématique à grande échelle d'une zone accessible au public*.

Dans ces cas-là, il faudra en principe toujours procéder à une AIPD préalable.

23. L'article 35(3)a du RGPD évoque des "*décisions*" produisant des effets juridiques à l'égard d'une personne physique ou l'affectant de manière significative de façon similaire. Il est important de faire remarquer qu'il n'est pas requis qu'il s'agisse d'une prise de décision "entièrement automatisée" au sens de l'article 22 du RGPD. Dès lors, l'article 35(3)a du RGPD s'applique aussi lorsque la prise de décision en question ne se base pas exclusivement sur un traitement automatisé[40].

24. Le RGPD ne définit pas ce que l'on entend par la notion de "*systématique*"[41]. "D'après le Groupe 29, cette notion doit être interprétée selon une ou plusieurs des manières qui suivent :

- une chose qui se déroule selon un système ;
- qui est préparée, organisée ou méthodique ;
- qui se déroule dans le cadre d'un plan général de collecte de données ;

[38] Groupe 29, Lignes directrices AIPD, p. 14-15.

[39] Voir plus haut, le point 10.

[40] Groupe Article 29, " Lignes directrices sur la prise de décision individuelle et le profilage automatisés aux fins du règlement 2016/679", WP251rev.01, 6 février 2018, p. 29.

[41] La Commission fait remarquer que dans la version anglaise et dans la version française du RGPD, tant à l'alinéa (a) qu'à l'alinéa (c), on utilise respectivement "systematic" et "systématique".

- qui est réalisée dans le cadre d'une stratégie[42].

25. Pour déterminer si le traitement est réalisé ou non "*à grande échelle*", il convient de considérer les facteurs suivants :

- le nombre de personnes concernées dont il s'agit (soit en valeur absolue, soit en proportion de la population considérée) ;
- le volume de données et/ou l'éventail des différents éléments de données traitées ;
- la durée ou la permanence du traitement de données ;
- de l'étendue géographique de l'activité de traitement[43].

Le considérant (91) du RGPD précise que l'obligation de conduire une analyse d'impact préalable ne s'applique pas aux traitements de données à caractère personnel de patients ou de clients effectués par un médecin, un autre professionnel de la santé ou un avocat exerçant à titre individuel. Dans de tels cas, le traitement ne peut être considéré comme étant à grande échelle.

26. Une "*zone accessible au public*" est un lieu, quel qu'il soit, ouvert à tout un chacun, tel qu'une place, un centre commercial, une rue, un marché, une gare ou encore une bibliothèque publique, par exemple[44].

27. Les **exemples** suivants illustrent les types de traitements visés par l'article 35(3) du RGPD :

a) Systèmes de suivi des élèves et e-learning

Il est question d'une "*évaluation systématique et approfondie d'aspects personnels concernant des personnes physiques*" au sens de l'article 35(3)a du RGPD lorsque le traitement vise à enregistrer de manière organisée plusieurs aspects personnels d'élèves (comme par exemple les connaissances, les prestations, les aptitudes sociales, l'état de santé mentale) et de les suivre de manière automatisée afin, sur cette base, de prendre des décisions quant à la suite du parcours de formation d'élèves individuels[45].

---

[42] *Ibid*, p. 11. À titre d'exemple d'activités considérées comme une observation régulière et systématique de personnes concernées, le Groupe 29 évoque notamment l'exploitation d'un réseau de télécommunications ou la fourniture de services de télécommunications ; le reciblage par courrier électronique ; le profilage et la notation à des fins d'évaluation des risques (par exemple, aux fins de l'évaluation du risque de crédit, de l'établissement des primes d'assurance, de la prévention de la fraude, de la détection du blanchiment d'argent).

[43] Groupe 29, Lignes directrices concernant les délégués à la protection des données, p. 9. À titre d'exemple d'un traitement à grande échelle, le Groupe 29 évoque notamment le traitement de données de patients par un hôpital dans le cadre du déroulement normal de ses activités ; le traitement de données à caractère personnel par un moteur de recherche à des fins de publicité comportementale, etc. (Ibid, p. 10). Dans le cas desdites applications de "big data", il sera aussi souvent question d'un traitement à grande échelle.

[44] Groupe de protection des données Article 29, Lignes directrices concernant la désignation d'une autorité de contrôle chef de file d'un responsable du traitement ou d'un sous-traitant", WP 244 rev.01, 5 avril 2017, p. 11.

[45] Pour un examen des risques en matière d'e-learning, voir également International Working Group on Data Protection in Telecommunications ("Berlin Group"), *Working Paper on E-Learning Platforms*, avril 2017, disponible à l'adresse https://www.datenschutz-berlin.de/pdf/publikationen/working-paper/2017/25042017_en_2.pdf.

b) Profils financiers

Il est également question d'une "*évaluation systématique et approfondie d'aspects personnels concernant des personnes physiques*" au sens de l'article 35(3)a du RGPD lorsque des données à caractère personnel de sources internes[46] et externes[47] sont réunies pour évaluer ou prédire la situation en matière de revenus ou de patrimoine, la solvabilité ou le modèle de dépenses de personnes concernées et lorsque ces informations sont prises en compte dans le cadre du service à la personne concernée ou de la décision de refuser ou de mettre fin à un service.

c) Systèmes d'information hospitaliers et recherche génétique

Il est question d'un "*traitement à grande échelle de catégories particulières de données*" au sens de l'article 35(3)b du RGPD lorsqu'un hôpital traite les données relatives à la santé de ses patients, ou lorsqu'un grand nombre de professionnels de la santé échangent de telles données via un plateforme commune[48]. Il en va de même lorsque les données génétiques d'un grand nombre de personnes concernées sont traitées ultérieurement à des fins scientifiques[49].

d) Vidéosurveillance

Il est question d'une "*surveillance systématique à grande échelle d'une zone accessible au public*" au sens de l'article 35(3)c du RGPD lorsqu'un exploitant ferroviaire instaure la vidéosurveillance dans toutes ses gares[50] ou lorsque l'on recourt régulièrement à une surveillance par caméras flexibles (par exemple) par les services de secours (par exemple au moyen de caméras installées sur les vêtements ou le casque de pompiers ou d'ambulanciers, de caméras sur le tableau de bord (ou dashcams)).

C) Les listes de l'autorité de contrôle

28. L'article 35(4) du RGPD oblige chaque autorité de contrôle à établir une liste des types d'opérations de traitement pour lesquelles une AIPD est requise et à communiquer ensuite cette liste au Comité européen de la protection des données (CEPD). Un projet de liste des types d'opérations de traitement pour lesquelles une AIPD est requise figure en annexe 2.

29. En outre, l'article 35(5) du RGPD permet également d'établir une liste des types d'opérations de traitement pour lesquelles aucune AIPD n'est requise. L'établissement d'une telle liste n'est pas obligatoire mais si elle est établie, elle doit être soumise au CEPD. Un projet de liste des types

[46] Par exemple la possession d'un produit, l'historique des transactions, les données de gestion de la relation client, les habitudes de navigation ou de clics, les données de localisation, etc.

[47] Par exemple les membres de la famille, les listes noires externes, les données achetées, etc.

[48] Voir aussi Groupe 29, Lignes directrices AIPD, p. 13 et Groupe 29, Lignes directrices concernant les délégués à la protection des données, p. 10.

[49] À cet égard, on rappelle qu'une seule AIPD peut porter sur un ensemble d'opérations de traitement similaires lorsqu'elles présentent des risques élevés similaires (article 35(1) du RGPD). Voir aussi plus haut, le point 92.

[50] Groupe 29, Lignes directrices AIPD, p. 8.

d'opérations de traitement qui sont dispensées de l'obligation de procéder à une AIPD figure en annexe 3.

30. La Commission souligne que les listes précitées ne portent **aucunement préjudice** à **l'obligation générale de gérer les risques** qui incombe au responsable du traitement, conformément à l'article 24(1) du RGPD[51]. Cette obligation générale d'évaluation et de maîtrise des risques vaut sans préjudice de l'existence d'une liste d'opérations de traitement particulières pour lesquelles la réalisation d'une AIPD est obligatoire (ni de l'existence d'une liste d'opérations de traitement pour lesquelles la réalisation d'une AIPD n'est pas obligatoire)[52]. De plus, les listes ne sont nullement exhaustives : une AIPD est toujours requise dès que les conditions d'application définies à l'article 35(1) du RGPD sont remplies.

31. Les projets de listes repris en annexes 2 et 3 doivent dès lors surtout être considérés comme des points de départ qui constituent une base supplémentaire lorsque le responsable du traitement cherche à vérifier si l'exécution d'une AIPD est requise.

4. À quel moment doit-on réaliser une AIPD ?

32.Lorsque la réalisation d'une AIPD est obligatoire, elle doit être réalisée **avant le traitement**[53]**.** Cette manière de faire est conforme au principe de protection des données dès la conception, qui requiert que le responsable du traitement, tant lors de la détermination des moyens du traitement que lors du traitement en lui-même, mette en œuvre des mesures techniques et organisationnelles appropriées, compte tenu des risques pour les droits et libertés de personnes physiques[54]. L'AIPD doit être considérée comme une aide à la prise de décision relative au traitement.

33. Une AIPD doit être lancée le plus tôt possible au cours de la conception du traitement (de préférence lorsque "l'idée de la création" d'un nouveau traitement survient), même si certains traitements ne sont pas encore connus. La mise à jour de l'AIPD tout au long du cycle de vie du projet permet de tenir compte de la protection des données et de la vie privée et stimule la création de solutions favorisant de manière générale le respect du RGPD[55], et en particulier l'obligation de protection des données dès la conception.

---

[51] Voir plus haut, le point 10.

[52] Voir aussi Groupe 29, Lignes directrices AIPD, p. 7.

[53] Article 35(1), 35(10) et considérants (90) et (93) du RGPD.

[54] Article 25(1) et considérant (78) du RGPD.

[55] Groupe 29, Lignes directrices AIPD, p. 17.

34. Il peut également être nécessaire de répéter certaines étapes de l'analyse au fur et à mesure de l'avancement du processus de développement, parce que la sélection de certaines mesures techniques et organisationnelles peut influencer la gravité ou la probabilité des risques engendrés par le traitement (par exemple une délégation d'une partie de l'activité de traitement à un sous-traitant). Le fait qu'une AIPD doive potentiellement être mise à jour après le commencement effectif du traitement n'est pas une raison valable de reporter l'analyse ou de ne pas la réaliser. La réalisation d'une AIPD est un **processus continu**, pas un exercice unique[56]. Cela sera d'autant plus important lorsqu'une activité ou un environnement de traitement est dynamique et est sujet à des changements permanents.

5. Quels sont les éléments essentiels d'une AIPD ?

A) Aperçu

35. L'article 35(7) du RGPD dispose qu'une AIPD doit au moins contenir les éléments suivants :

> "*a) une description systématique des opérations de traitement envisagées et des finalités du traitement, y compris, le cas échéant, l'intérêt légitime poursuivi par le responsable 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 conformément au paragraphe 1 ; et*
>
> *d) les mesures envisagées pour faire face aux risques, y compris les garanties, mesures et mécanismes de sécurité 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*."

B) Description des opérations de traitement envisagées et des finalités du traitement

36. L'article 35(7) du RGPD exige en premier lieu que l'AIPD contienne une *description systématique* des opérations de traitement envisagées et des finalités du traitement. Il est important que l'on tienne compte à cet égard de la nature, de la portée, du contexte et des finalités du traitement et des sources des risques[57]. La description doit comporter **au moins les éléments suivants** :

- une description claire du traitement, y compris d'éventuels processus d'entreprise et exigences du système ;

[56] Groupe 29, Lignes directrices AIPD, p. 17-18.

[57] Voir également le considérant (90) du RGPD.

- les données à caractère personnel, les destinataires et la durée pendant laquelle les données à caractère personnel seront enregistrées ;
- les actifs sur lesquels reposent les données à caractère personnel (par exemple matériels, logiciels, réseaux, personnes, documents papier ou canaux de transmission papier)[58].

Parmi d'autres éléments pertinents pour déterminer la nature, la portée et le contexte des traitements, on peut citer : les catégories de personnes concernées, l'échelle du traitement de données, l'origine des données, la relation entre le responsable du traitement et les personnes concernées, les éventuelles conséquences pour les personnes concernées et le degré de facilité avec lequel on peut identifier les personnes concernées.

37. Le responsable du traitement doit veiller à ce que les opérations de traitement et finalités du traitement visées soient décrites avec la précision nécessaire. On ne peut se contenter de se référer à des finalités générales, décrites au sens large (comme par exemple "améliorer l'expérience d'utilisateur", "sécurité IT", "recherche")[59]. Cela s'applique *mutatis mutandis* à l'égard des traitements visés. La description doit donner au lecteur une idée claire des traitements de données visés par le responsable du traitement. La Commission recommande également de décrire de manière suffisamment détaillée et claire les moyens du traitement. Une visualisation des traitements envisagés peut contribuer à favoriser une approche systématique[60]. Enfin, il est également important que le responsable du traitement décrive clairement quels sont ses intérêts légitimes (ou ceux d'éventuels tiers), en particulier si le traitement est basé sur l'article 6(1)f du RGPD[61].

C) Contrôle de la proportionnalité

38. Une AIPD doit comporter une évaluation de la **nécessité et de la proportionnalité** des opérations de traitement au regard des finalités. Le responsable du traitement doit dès lors justifier explicitement (1) pour quelle(s) raison(s) le traitement de données à caractère personnel est nécessaire et (2) pour quelle(s) raison(s) chacun des traitements visés est nécessaire pour atteindre

---

[58] Groupe 29, Lignes directrices AIPD, p. 28.

[59] Voir également l'Article 29 Data Protection Working Party, "Opinion 03/2013 sur la limitation de la finalité", 2 avril 2013, pp. 15-16. La description des finalités du traitement et des activités de traitement doit toujours être suffisamment détaillée pour permettre une appréciation correcte des risques, en fonction de la nature, de la portée, du contexte et des finalités du traitement. Pour la description des finalités des traitements envisagés, la liste des finalités mentionnée dans la notice explicative de la déclaration préalable, élaborée dans le contexte de l'article 17 de la loi vie privée, peut être utile. Voir Commission de la protection de la vie privée, "Notice explicative – Déclaration ordinaire", 2007, disponible à l'adresse https://www.privacycommission.be/sites/privacycommission/files/documents/notice_decl_ordinaire_0.pdf. Voir également Commission de la protection de la vie privée, Recommandation n° 06/2017 du 14 juin 2017 relative au Registre des activités de traitements (article 30 du RGPD), p. 11 e.s.

[60] Une description précise et systématique des traitements envisagés constitue non seulement un avantage pour le lecteur, mais aussi une condition essentielle pour la bonne réalisation d'une AIPD. Ce n'est qu'avec une description précise que l'on peut déterminer les mesures recommandées pour limiter les risques.

[61] Voir aussi par exemple ISO/IEC 29134, "Information technology – Security Techniques – Guidelines for privacy impact assessment, 2017, p. 10-11 et 13-14 ; Rijksoverheid, Model PIA, p. 15 et CNIL, Privacy Impact Assessment (PIA) Tools (templates and knowledge bases), 2015, p. 4-6. La désignation des intérêts légitimes peut aussi, le cas échéant, se faire dans le cadre du contrôle de la proportionnalité. Voir ci-après, le point 40

la (les) finalité(s) poursuivie(s). Si plusieurs traitements ou moyens de traitement sont utilisés pour atteindre la (les) finalité(s), le responsable du traitement doit en principe choisir les moyens de traitement qui sont les moins intrusifs[62]. Le responsable du traitement a alors intérêt à bien documenter la (les) raison(s) pour laquelle (lesquelles) les moyens de traitement choisis sont moins intrusifs que les alternatives.

39. Lors de l'évaluation de la proportionnalité, le responsable du traitement doit également examiner la **pertinence** du traitement envisagé (peut-on raisonnablement espérer que le traitement envisagé atteindra sa finalité (légitime) ?)[63]. Enfin, le responsable du traitement doit aussi veiller à maintenir un **équilibre adéquat** entre les intérêts pertinents[64].

40. Par conséquent, lors de l'évaluation de la nécessité et de la proportionnalité du traitement envisagé, il faut tenir compte **au moins des éléments suivants** :

- la (les) finalité(s) spécifiée(s), explicite(s) et légitime(s) du traitement envisagé ;
- le fondement juridique sur lequel se base le traitement de données (article 6 du RGPD)[65];
- une justification du fait que les données à caractère personnel traitées sont adéquates, pertinentes et limitées à ce qui est nécessaire (article 5(1)c du RGPD) ;
- une justification du délai de conservation envisagé des données à caractère personnel, qui ne peuvent être conservées sous une forme permettant l'identification des personnes concernées que pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées (article 5(1)e) du RGPD[66];
- une justification du fait que les intérêts de la personne concernée ne prévalent pas sur les intérêts légitimes du responsable du traitement ou d'éventuels tiers.

41. Enfin, il est également recommandé que le responsable du traitement propose un relevé de toutes les mesures prises pour remplir les obligations du RGPD[67]. Cela permettra en premier lieu au

---

[62] Voir également Rijksoverheid, Model PIA, p. 16.

[63] Voir également l'article 5(1)c du RGPD (les données à caractère personnel doivent être "*adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (minimisation des données)*)".

[64] L'évaluation de l'équilibre d'intérêts à ce stade de l'AIPD ne sera généralement que provisoire, étant donné qu'elle ne tient pas encore compte des mesures de protection visées (cf. ci-dessous aux points 56e.s.). Voir aussi Groupe 29, Lignes directrices AIPD, p. 28.

[65] En principe, une opération de traitement qui ne poursuit qu'une seule finalité ne peut être justifiée qu'à l'aide d'un seul des fondements juridiques repris à l'article 6 du RGPD. Il est toutefois possible qu'un même traitement poursuive plusieurs finalités. Dans ce cas, il est possible que plus d'un fondement juridique entre en considération pour justifier le traitement de données envisagé. Voir Groupe de protection des données Article 29, Guidelines for consent under 2016/679, WP 259, 28 novembre 2017, p. 22.

[66] Groupe 29, Lignes directrices AIPD, p. 28.

[67] À ce stade du RGPD, il n'est pas exigé que ces mesures soient décrites, le responsable du traitement peut aussi choisir de les reprendre à un stade antérieur (par exemple lors de la description du traitement de données envisagé) ou dans un document distinct.

responsable du traitement de prouver que le RGPD a été respecté[68]. Ensuite, ces mesures auront aussi évidemment un impact sur l'évaluation ultérieure des risques[69]. La Commission s'attend ainsi à ce qu'une AIPD fournisse également un aperçu :

- des mesures qui contribuent aux droits des personnes concernées, dont :
    - l'information communiquée à la personne concernée (articles 12, 13 et 14 du RGPD) ;
    - le droit d'accès et le droit à la portabilité des données (articles 15 en 20 du RGPD) ;
    - le droit de rectification et le droit à l'effacement de données (articles 16, 17 et 19 du RGPD) ;
    - le droit d'opposition et le droit à la limitation du traitement (articles 18, 19 et 21 du RGPD) ;
- de la manière dont les relations avec les sous-traitants sont régies (article 28 du RGPD) ;
- des garanties concernant le (les) transfert(s) international (internationaux) qui seront prévues le cas échéant (chapitre V du RGPD)[70].

D) Évaluation des risques

- *Qu'est-ce qu'une "évaluation des risques" ?*

42. La notion d' "évaluation des risques" renvoie à l'ensemble du processus (1) d'identification des risques, (2) d'analyse des risques et (3) d'évaluation des risques[71]. **L'identification** des risques renvoie au processus visant à examiner, reconnaître et décrire les risques[72]. L'**analyse** du risque renvoie au processus mis en œuvre pour comprendre la nature d'un risque et pour déterminer le niveau de risque[73]. L'**évaluation** du risque est le processus de comparaison des résultats de l'analyse du risque avec les critères de risque préétablis afin de déterminer si le risque (et/ou son importance) est (sont) acceptable(s) ou tolérable(s)[74].

43. En matière de gestion des risques, on peut en règle générale faire une distinction entre le risque "inhérent" et le risque "résiduel". Le risque "**inhérent**" renvoie à la probabilité qu'un impact négatif

---

[68] Article 37(7)d du RGPD.

[69] Voir ci-après, le point 42

[70] Groupe 29, Lignes directrices AIPD, p. 28.

[71] ISO, "Risk management – Vocabulary", ISO Guide 73:2009. Lors de l'identification des risques, le responsable du traitement doit faire preuve de la prudence nécessaire et anticiper les risques potentiels, même si la nature du risque n'est pas connue à l'avance. L'évaluation du niveau de risque n'a en effet lieu que lors de l'analyse ultérieure des risques identifiés.

[72] *Id.* L'identification des risques comporte l'identification de la source des risques, d'événements, de leurs causes et de leurs éventuelles conséquences.

[73] *Id.*

[74] *Id.*

se produise lorsqu'aucune mesure de protection n'est prise[75]. Le risque "**résiduel**" " renvoie au contraire à la probabilité qu'un impact négatif se produise, malgré les mesures qui sont prises pour influencer (limiter) le risque (inhérent)[76].

44. Au moment de l'exécution de l'AIPD, le responsable du traitement qui la réalise aura déjà pris plusieurs mesures pour respecter les obligations du RGPD. Ces **mesures existantes** peuvent avoir une influence sur l'évaluation des risques pour les droits et libertés des personnes physiques. Il est dès lors important que celles-ci soient documentées, afin qu'elles puissent aussi être prises en compte lors de l'évaluation et de la détermination des risques résiduels finaux[77].

- *De quels risques s'agit-il ?*

45. L'article 35(1) du RGPD ne renvoie pas uniquement au droit à la vie privée ou au droit à la protection des données, mais aussi aux risques pour les droits et libertés des personnes physiques en général[78]. Des risques pertinents peuvent aussi le cas échéant se rapporter à d'autres droits et libertés fondamentaux, comme par exemple la liberté de parole, la liberté de pensée, la liberté de conscience et de religion, l'interdiction de toute discrimination et la liberté de circulation[79].

46. Le traitement de données à caractère personnel peut comporter plusieurs risques pour les droits et libertés des personnes physiques. Le considérant (75) du RGPD donne plusieurs **exemples** (non limitatifs) de conséquences négatives pour les droits et libertés des personnes physiques qui peuvent se produire lors d'un traitement de données à caractère personnel, à savoir :

- la discrimination ;
- un vol d'identité ou une fraude à l'identité ;
- des pertes financières ;
- une atteinte à la réputation ;
- une perte de confidentialité de données à caractère personnel protégées par le secret professionnel ;
- la suppression non autorisée de la pseudonymisation ;

---

[75] Lors de l'analyse (évaluation) du risque, on tient compte de la présence (ou de l'absence) et de l'efficacité de mesures techniques et organisationnelles qui limitent le risque. IEC/ISO, "Risk management – Risk management techniques", IEC/ISO 31010, v1.0, 2009-11, p. 12. Voir également le schéma du Groupe 29, Lignes directrices AIPD, p. 20.

[76] Voir également ISO, "Risk management – Vocabulary", ISO Guide 73:2009, qui décrit le "risque résiduel" comme "*risque subsistant après le traitement du risque*"). Il est important de faire remarquer qu'il est en principe impossible d'exclure totalement les risques. Il restera toujours un risque résiduel. Le responsable du traitement doit décrire comment il en est arrivé à ce risque résiduel et pourquoi il l'estime acceptable. (Rijksoverheid, Model PIA, p. 37.) Voir également ci-après, le point 59.

[77] Voir plus haut, le point 41. Le responsable du traitement choisit en principe librement l'endroit de l'AIPD où ces mesures sont documentées.

[78] Voir aussi les considérants (74) à (77) inclus du RGPD.

[79] Groupe 29, Lignes directrices AIPD, p. 7.

- la situation où des personnes concernées ne peuvent pas exercer leurs droits et libertés ou sont empêchées d'exercer le contrôle sur leurs données à caractère personnel ; et
- tout autre dommage économique ou social important[80].

On peut également citer comme **exemples** de conséquences négatives potentielles pour les droits et libertés des personnes concernées :

- la perte d'une opportunité ;
- l'atteinte portée à la tranquillité ou au bien-être ;
- la stigmatisation ou le stéréotypage ;
- le refus ou la limitation d'accès à des lieux ou événements qui sont d'habitude accessibles au public ;
- le traitement déloyal (par exemple fixation des prix différenciée) ;
- la manipulation (par exemple l'exploitation d'émotions) ;
- l'adaptation de comportement (par exemple autocensure) ; et
- l'atteinte portée à l'intégrité physique ou morale[81].

- *Besoin d'une analyse contextuelle*

47. Tous les traitements de données à caractère personnel ne donnent pas lieu aux mêmes risques. De plus, la gravité et/ou la probabilité d'un risque peut fortement varier en fonction de chaque traitement. L'analyse des risques doit toujours se faire en fonction de l'ensemble des circonstances particulières de chaque traitement (ou groupe d'opérations de traitement similaires[82]). Ainsi, le considérant (76) du RGPD dispose ce qui suit :

> "*Il convient de déterminer la probabilité et la gravité du risque pour les droits et libertés de la personne concernée <u>en fonction</u> de la nature, de la portée, du contexte et des finalités du traitement*."

C'est donc en fonction de l'ensemble des circonstances particulières de chaque traitement que le responsable du traitement doit évaluer les risques pour les droits et libertés des personnes et doit prendre les mesures appropriées pour garantir l'application des dispositions du RGPD[83].

---

[80] Le considérant (75) du RGPD évoque par ailleurs aussi plusieurs éléments qui peuvent avoir un effet d'accroissement des risques. Ces éléments ont déjà été évoqués dans la section 3, étant donné qu'ils ont été traités dans les 9 critères du Groupe 29. Voir plus haut, le point 19

[81] Voir aussi Groupe de protection des données Article 29, Lignes directrices concernant la désignation d'une autorité de contrôle chef de file d'un responsable du traitement ou d'un sous-traitant, WP 244 rev.01, 5 avril 2017, p. 4 (exemples de conséquences qui "affectent sensiblement" au sens de l'article 4(23) du RGPD).

[82] Conformément à l'article 35(1) du RGPD, une seule AIPD peut porter sur un ensemble d'opérations de traitement similaires qui présentent des risques élevés similaires (voir ci-après le point 92).

[83] Comme indiqué précédemment, les éléments suivants sont pertinents pour déterminer la nature, la portée et le contexte des traitements : les données à caractère personnel, les destinataires et la durée pendant laquelle les données à caractère personnel sont conservées, les catégories de personnes concernées, l'échelle du traitement de données, l'origine des données, la relation entre le responsable du traitement et les personnes concernées, et le niveau de facilité avec lequel on peut identifier les personnes concernées. Voir plus haut, le point 36.

48. L'évaluation des risques implique de cerner la probabilité et la gravité du risque. Lors de **l'évaluation** du risque, le responsable du traitement doit se poser les questions suivantes : quelle est l'ampleur de l'impact potentiel sur les personnes concernées et quelle est la probabilité que cet impact se produise ? Il n'est pas toujours possible de répondre de manière bien tranchée à ces questions, il s'agira souvent en pratique d'une pondération qui permettra de déterminer le **niveau de risque**[84]**.**

49. Lors de l'évaluation des risques, il est important de tenir compte de l'origine, de la nature, de la particularité et de la gravité des risques en question[85]. Cela implique en particulier d'établir, pour chaque risque, **au moins les éléments suivants** :

- les sources des risques[86];
- les impacts potentiels sur les droits et libertés des personnes concernées, en particulier en cas d'événements tels qu'un accès illicite aux données, une modification non désirée ou leur disparition ;
- les menaces qui pourraient conduire à un accès illégitime aux données, à une modification non désirée de celles-ci ou à leur disparition ; et
- la probabilité et la gravité du risque[87].

50. Les considérants (84) et (90) du RGPD précisent que l'AIPD vise en premier lieu les risques "élevés". Si par exemple lors d'un traitement déterminé, il y a un risque élevé d'atteinte à la réputation mais qu'il n'y a qu'un très faible risque de discrimination, ce dernier risque ne doit pas nécessairement être repris en tant que tel dans l'évaluation des risques d'une AIPD. Néanmoins, la Commission recommande, dans le cadre d'une AIPD, de cartographier expressément tous les risques qui ne sont pas négligeables et d'identifier des mesures de protection efficaces, étant donné que même des risques moyens peuvent constituer un facteur important lors de l'évaluation de la proportionnalité du traitement de données envisagé[88]. En outre, la réalisation d'une AIPD ne dispense pas le responsable du traitement de son obligation générale de prendre des mesures pour gérer de manière appropriée tous les risques pour les droits et libertés des personnes concernées. Enfin, une AIPD doit quoi qu'il en soit comporter un relevé de toutes les mesures prises afin d'apporter la preuve du respect du RGPD, compte tenu des droits et des intérêts légitimes des personnes concernées et des autres personnes

[84] Rijksoverheid, Model PIA, p. 36.

[85] Voir le considérant (84) du RGPD.

[86] Voir le considérant (90) du RGPD.

[87] Groupe 29, Lignes directrices AIPD, p. 28.

[88] Voir plus haut, les points 38 e.s.

affectées[89]. Dans cette optique également, il est important que tous les risques pertinents soient pris en compte.

- *Quelle méthode faut-il appliquer lors de l'évaluation et de la gestion des risques ?*

51. Le responsable du traitement peut choisir librement la méthode qu'il souhaite appliquer, à condition qu'elle mène à une **évaluation objective** du risque[90] et qu'elle tienne compte des **éléments minimaux** que prescrit le RGPD. Il appartient au responsable du traitement d'utiliser une méthode qui lui permet de respecter les exigences du RGPD. Cela signifie également que le choix de l'une ou l'autre méthode doit pouvoir être justifié, compte tenu de la nature, du champ d'application, du contexte et des finalités du traitement.

52. Néanmoins, la Commission estime qu'une bonne gestion des risques présente **plusieurs caractéristiques minimales** qui sont énumérées dans l'annexe 1 de la présente recommandation.

53. La Commission estime important que chaque responsable du traitement qui entreprend une AIPD utilise une méthode qui soit adaptée aux besoins et au contexte de sa propre entreprise. La nécessité d'une analyse contextuelle n'empêche pas qu'un responsable du traitement recoure à des procédures ou modèles standardisés qui ont été élaborés par (ou en collaboration avec) d'autres entités (par exemple au niveau d'un secteur ou d'une branche d'activités déterminé(e)) pour la réalisation d'une évaluation des risques.

54. En outre, la Commission recommande vivement que le responsable du traitement se base sur des méthodes déjà existantes en matière de gestion des risques. L'utilisation de normes internationales, telles que celles développées par l'Organisation internationale de normalisation (ISO)[91], ainsi que de codes de conduite élaborés ou agréés au niveau européen, est particulièrement importante dans ce cadre[92].

55. Quelle que soit la méthode finalement retenue par le responsable du traitement, la Commission estime indispensable que ce dernier indique explicitement quelle méthode a été choisie et que celle-ci soit appliquée de manière cohérente tout au long du processus de l'AIPD.

---

[89] Article 35(7)d du RGPD. Voir ci-après, les points 56 e.v.

[90] Le considérant (76) du RGPD confirme le caractère objectif de cette évaluation du risque à l'égard du traitement et des conséquences de celui-ci pour les droits et libertés des personnes : "*Le risque devrait faire l'objet d'une évaluation objective* permettant de déterminer si les opérations de traitement des données comportent un risque ou un risque élevé."

[91] En particulier la norme ISO 31000 (Risk management). ISO 27005 (Information security risk management) et ISO/IEC 29134 (Guidelines for privacy impact assessment). Comme indiqué plus haut, tout responsable du traitement reste en principe libre de choisir la méthode à employer. Le responsable du traitement n'est dès lors pas obligé d'utiliser une norme déterminée (internationale ou autre), ni de désigner une personne qui est certifiée pour réaliser une AIPD selon ladite norme.

[92] En ce qui concerne les codes de conduite agréés ou élaborés au niveau européen, voir également ci-après les points 94 e.s.

E) Mesures visées

56. Une AIPD ne comprend pas uniquement une évaluation des risques mais aussi un relevé des mesures visées afin **de faire face aux risques**, dont les garanties, les mesures de sécurité et les mécanismes pour assurer la protection des données à caractère personnel et pour démontrer que le RGPD a été respecté[93].

57. Les mesures pertinentes peuvent être de nature aussi bien technique, qu'organisationnelle ou juridique, comme par exemple :

- *mesures organisationnelles* : accroissement de la conscientisation, formation, mesures politiques, séparation des fonctions (ce qu'on appelle "Muraille de Chine"), rapport, contrôles périodiques, possibilités supplémentaires de choix, de participation ou d'opposition pour les personnes concernées, etc.
- *mesures techniques* : limitations techniques à la collecte et/ou à la communication de données à caractère personnel (par exemple utilisation de techniques cryptographiques particulières pour faire de la minimalisation de données), l'anonymisation, la pseudonymisation et/ou le cryptage de données à caractère personnel après leur collecte, les limitations techniques à la réutilisation de données à caractère personnel (finalité), l'authentification multifacteurs, la journalisation et le monitoring, la scission de données, les sauvegardes supplémentaires, etc.
- *mesures juridiques* : garanties contractuelles, règles d'entreprise contraignantes, etc[94].

58. Lorsque le traitement de données envisagé recourt au profilage ou à ce qu'on appelle les analyses "big data", le risque de traitement de données inexactes et/ou de discrimination indirecte peut augmenter. Dans de tels cas, le responsable du traitement doit recourir à des procédures mathématiques et statistiques appropriées et prendre des mesures techniques et organisationnelles qui permettent de corriger les facteurs induisant des inexactitudes dans les données à caractère personnel et de minimaliser le risque d'erreurs[95]. Le responsable du traitement doit en outre éviter que le traitement ait des conséquences discriminantes sur la base de l'origine raciale ou ethnique, des opinions politiques, de la religion ou des convictions, de l'appartenance syndicale, du statut génétique ou de l'état de santé, ou de l'orientation sexuelle, ou ait des conséquences qui se traduisent par des mesures produisant un tel effet[96]. Pour éviter de telles conséquences, il convient également de vérifier

---

[93] Article 35(7)d du RGPD.

[94] Voir également ci-après Commission Informatique et Libertés, CNIL, Measures for the privacy risk treamtent – Good Practices Catalogue, 2012, 92 p.; Information Commissioner's Office (ICO), Conducting privacy impact assessments – code of practice, p. 27-30 et Rijksoverheid, Model PIA, p. 37-38.

[95] Considérant (71) du RGPD.

[96] Idem. Voir également ci-après Commission de la protection de la vie privée, Rapport Big Data, 2017, p. 19-31 et Rijksoverheid, Model PIA, p. 39.

s'il existe une possibilité qu'un risque déterminé soit fortement susceptible de se produire chez certaines minorités ou groupes protégés.

59. Dans le cadre de l'évaluation des mesures visées afin de faire face aux risques, le responsable du traitement doit s'assurer que les droits et intérêts légitimes des personnes concernées et des autres personnes sont dûment respectés[97]. À cet égard, il faut toujours garder une vue d'ensemble à l'esprit : la nature, la portée, le contexte et la finalité du traitement, les risques, l'état de la technique et les frais d'exécution[98]. Plus les risques sont élevés, plus grandes seront les attentes à l'égard du responsable du traitement quant aux mesures à prendre. Le responsable du traitement ne doit donc pas toujours prendre toutes les mesures possibles. Le RGPD exige uniquement que les mesures ramènent les risques à un niveau acceptable et qu'il y ait un équilibre adéquat entre les mesures envisagées et les risques en cause[99].

60. Le coût des mesures envisagées ne peut pas en soi constituer une raison de réaliser un traitement sans garanties suffisantes. Si le responsable du traitement n'est pas en mesure de prévoir des garanties suffisantes et de ramener le risque à un niveau acceptable, au vu de la technologie disponible et des frais d'exécution, il doit le cas échéant soit renoncer au traitement, soit réaliser une consultation préalable de l'autorité de contrôle[100].

61. Lors de l'identification des mesures envisagées, le responsable du traitement doit indiquer explicitement quelles mesures servent à limiter quels risques. À cet égard, il est recommandé que le responsable du traitement précise aussi expressément :

- quels moyens seront nécessaires pour mettre en œuvre les mesures ;
- quelle(s) personne(s) sera (seront) responsable(s) de la mise en œuvre de ces mesures ;
- la durée au cours de laquelle les mesures seront exécutées ;
- la manière dont la pertinence des mesures sera contrôlée et évaluée[101].

6. Quand une consultation préalable est-elle requise ?

62. L'article 36(1) du RGPD dispose que :

---

[97] Article 35(7)d du RGPD *in fine*.

[98] Voir également les articles 25(1) et 32(1) du RGPD.

[99] Rijksoverheid, Model PIA, p. 37. Il est également important de faire remarquer qu'il est en principe impossible d'exclure totalement les risques. Il restera toujours un risque résiduel. Le responsable du traitement doit décrire comment il en est arrivé à ce risque résiduel et pourquoi il l'estime acceptable. (*Id.*)

[100] Considérant (84) du RGPD. Voir ci-après le point 63.

[101] ISO/IEC 29134, "Information technology – Security techniques – Guidelines for privacy impact assessment", 2017, p. 23. En ce qui concerne la gestion et la vérification de l'AIPD, voir ci-après le point 96

"Le responsable du traitement consulte l'autorité de contrôle préalablement au traitement lorsqu'une analyse d'impact relative à la protection des données effectuée au titre de l'article 35 indique que le traitement présenterait un risque élevé si le responsable du traitement ne prenait pas de mesures pour atténuer le risque."

63. Il ressort de la formulation de l'article 36(1) du RGPD qu'une consultation préalable n'est obligatoire que lorsque le risque *résiduel* est élevé[102]. Une consultation préalable n'est donc requise que lorsque l'AIPD démontre que le traitement va de pair avec un risque élevé que le responsable du traitement ne peut atténuer en prenant des mesures appropriées compte tenu des techniques disponibles et des coûts liés à leur mise en œuvre[103]. Si le risque peut être limité efficacement à l'aide de mesures techniques et organisationnelles appropriées, aucune consultation préalable ne doit avoir lieu[104].

64. Un risque résiduel élevé inacceptable existe par exemple lorsqu'il est probable que les personnes concernées soient confrontées à des conséquences considérables ou irréversibles (par exemple un accès illégitime à leurs données qui pourrait menacer leur vie, entraîner une mise à pied, mettre en péril leur situation financière). Il semble ainsi évident que le risque se concrétisera dans la mesure où il n'est pas possible de réduire le nombre de personnes accédant aux données en raison de leurs modes de partage, d'utilisation ou de distribution, ou en présence d'une vulnérabilité bien connue non corrigée[105].

65. Si l'autorité de contrôle estime que le traitement envisagé n'est pas conforme au RGPD ou que les risques ne sont pas suffisamment identifiés ou atténués, elle fournit, dans un délai maximum de huit semaines à compter de la réception de la demande de consultation, un avis écrit au responsable du traitement et, le cas échéant, au sous-traitant, et peut faire usage des pouvoirs visés à l'article 58 du RGPD, y compris le pouvoir d'imposer une limitation temporaire ou définitive, y compris une interdiction, du traitement[106]. Ce délai de 8 semaines peut être prolongé de 6 semaines[107]. Ces délais peuvent être suspendus jusqu'à ce que l'autorité de contrôle ait obtenu les informations qu'elle a demandées pour les besoins de la consultation (article 36(2) du RGPD).

---

[102] L'article 35(1) du RGPD concerne, contrairement à l'article 36(1) du RGPD, le risque "inhérent" du traitement de données envisagé. Voir aussi Groupe 29, Lignes directrices AIPD, p. 10. En ce qui concerne la distinction entre les risques "inhérents" et les risques "résiduels", voir ci-dessus le point 43.

[103] Considérant (84) du RGPD.

[104] Groupe 29, Lignes directrices AIPD, p. 23.

[105] Groupe 29, Lignes directrices AIPD, p. 23.

[106] Article 58(2)e du RGPD.

[107] Dans le cas d'une telle prolongation, l'autorité de contrôle informe le responsable du traitement et, le cas échéant, le sous-traitant de la prolongation du délai ainsi que des motifs du retard notamment, dans un délai d'un mois à compter de la réception de la demande de consultation.

66. Lorsqu'une consultation préalable est obligatoire, le responsable du traitement fournit les informations suivantes (article 36(3) du RGPD) :

a) le cas échéant, les responsabilités respectives du responsable du traitement, des responsables conjoints et des sous-traitants participant au traitement, en particulier pour le traitement au sein d'un groupe d'entreprises ;

b) les finalités et les moyens du traitement envisagé ;

c) les mesures et les garanties prévues afin de protéger les droits et libertés des personnes concernées en vertu du RGPD ;

d) le cas échéant, les coordonnées du délégué à la protection des données ;

e) l'analyse d'impact relative à la protection des données prévue à l'article 35 du RGPD ; et

f) toute autre information demandée par l'autorité de contrôle.

7. Qui assure quel rôle lors de l'exécution d'une AIPD ?

A) Le(s) responsable(s) du traitement

67. L'obligation de procéder à une AIPD incombe en premier lieu au responsable du traitement. Il est celui qui endosse la responsabilité finale et est responsable si l'AIPD n'est pas (ou pas correctement) réalisée lorsque celle-ci est bel et bien obligatoire en vertu de l'article 35 du RGPD. L'AIPD peut être réalisée par quelqu'un d'autre, à l'intérieur ou à l'extérieur de l'organisation, mais le responsable du traitement reste responsable en dernier ressort de cette tâche[108].

68. La Commission estime indispensable que le responsable du traitement veille à ce que les bonnes personnes au sein de l'entreprise soient impliquées dans le processus d'évaluation des risques[109]. Afin d'éviter que le processus d'évaluation des risques soit ramené à un pur exercice écrit, ceux qui sont les mieux placés pour contribuer à une évaluation des risques de qualité doivent être impliqués en temps opportun dans le processus d'identification, d'évaluation et de gestion des risques. La Commission pense ici en premier lieu non seulement au délégué à la protection des données et/ou au conseiller en sécurité, mais aussi aux concepteurs de nouvelles applications (par exemple des architectes ICT), aux analystes, aux juristes d'entreprises, aux personnes qui prennent des décisions stratégiques en matière de développement de projets, aux responsables de la sous-traitance, aux

[108] Groupe 29, Lignes directrices AIPD, p. 18.

[109] Voir également l'annexe 1, point 6.

responsables de la gestion du personnel, aux membres du personnel (ou à leurs représentants) qui utiliseront les données à caractère personnel en question dans l'exercice de leurs tâches, etc.[110]

69. Décrire et documenter les tâches et responsabilités spécifiques des personnes au sein de l'entreprise constitue une bonne pratique, en tenant compte de la politique, des processus et des règles internes. Par exemple :

- en cas de proposition faite par une unité opérationnelle spécifique de procéder à une AIPD, l'unité en question devrait ensuite contribuer à l'AIPD et devrait être impliquée dans le processus de validation de l'analyse ;
- le cas échéant, il est recommandé de recueillir les conseils d'experts indépendants de différentes professions (avocats, experts en informatique, experts en sécurité, sociologues, experts en déontologie, etc.) ;
- le responsable de la sécurité des systèmes d'information (RSSI), si un tel responsable a été désigné, ainsi que le DPD, peuvent être amenés à suggérer au responsable du traitement d'effectuer une AIPD sur une opération de traitement spécifique et devraient dès lors apporter leur appui aux parties prenantes en ce qui concerne la méthodologie à suivre, participer à l'évaluation de la qualité de l'analyse des risques et de l'acceptabilité des risques résiduels, et contribuer au développement des connaissances spécifiques au contexte du responsable du traitement ;
- le responsable de la sécurité des systèmes d'information (RSSI), si un tel responsable a été désigné, et/ou le service informatique, devraient apporter leur assistance au responsable du traitement et peuvent être amenés à proposer la réalisation d'une AIPD sur une opération de traitement spécifique, en fonction des besoins en matière de sécurité ou des besoins opérationnels[111].

70. Si le responsable du traitement a désigné un délégué à la protection des données, il est quoi qu'il en soit obligé de lui demander conseil[112], et ce conseil doit être documenté dans l'AIPD, conjointement avec les décisions du responsable du traitement[113]. Le délégué à la protection des données doit également vérifier l'exécution de l'AIPD[114].

---

[110] Il est recommandé de documenter expressément la tâche et le rôle de chacune de ces personnes lors de la réalisation (de parties) d'une AIPD. Pour un exemple de présentation de cette répartition, voir Commission Nationale de l'Informatique et des Libertés (CNIL), "Privacy Impact Assessment (PIA) - Methodology (how to carry out a PIA)", 2015, p. 9.

[111] Groupe 29, Lignes directrices AIPD, p. 19.

[112] Article 35(2) du RGPD.

[113] Groupe 29, Lignes directrices AIPD, p. 18.

[114] Article 39(1)c du RGPD. Voir également ci-après le point 76.

71. En outre, la Commission recommande aussi que les décisions finales prises dans le cadre d'une AIPD le soient à un niveau hiérarchique suffisamment élevé. L'approbation d'une AIPD ou la décision de ne pas procéder à une AIPD pourrait par exemple être officiellement soumise à l'aval des membres de la direction ou d'un organe interne mandaté[115]. Étant donné que la réalisation d'une AIPD n'est obligatoire que lorsqu'il est question d'un traitement susceptible d'engendrer un risque élevé pour les droits et libertés fondamentaux des personnes physiques, il est logique que les décisions à l'égard d'une AIPD soient expressément prises directement ou indirectement par l'organe le plus élevé de l'entreprise.

72. Lorsque l'opération de traitement implique des responsables conjoints du traitement, ceux-ci doivent définir précisément leurs obligations respectives. Il convient que leur AIPD détermine quelle partie est responsable des différentes mesures destinées à faire face aux risques et à protéger les droits et libertés des personnes concernées, et que chaque responsable du traitement exprime ses besoins et partage les informations utiles en veillant à ne pas compromettre de secrets (secrets d'affaires, propriété intellectuelle, informations commerciales confidentielles, par exemple) et à ne pas divulguer de vulnérabilités[116].

B) Le sous-traitant

73. Le sous-traitant doit, en fonction de la nature du traitement, assister le responsable du traitement dans l'exécution d'une AIPD. Dans les précédentes versions du projet du RGPD, il était même explicitement prévu que l'obligation de procéder à une AIPD en tant que telle reposerait également directement sur le sous-traitant. Dans la version finale du RGPD, il est toutefois précisé que le *contrat* entre le responsable du traitement et le sous-traitant doit établir que le sous-traitant :

> "*aide le responsable du traitement à garantir le respect des obligations prévues aux articles 32 à 36, compte tenu de la nature du traitement et des informations à la disposition du sous-traitant*"[117].

74. Le considérant (95) du RGPD confirme que le sous-traitant doit aider le responsable du traitement, "si nécessaire et sur demande", à assurer le respect des obligations découlant de la réalisation d'une AIPD et d'une consultation préalable de l'autorité de contrôle.

75. Compte tenu des dispositions précitées, l'ampleur de l'obligation d'assistance du sous-traitant doit être déterminée à la lumière (1) de la nature du traitement ; (2) des informations mises à disposition

[115] Voir également annexe 1, point 7.

[116] Groupe 29, Lignes directrices AIPD, p. 8.

[117] Article 28(3)f du RGPD.

du sous-traitant ; (3) de l'opportunité de l'aide du sous-traitant afin de parvenir à une analyse et à une gestion des risques correctes et de qualité.

C) Le délégué à la protection des données

76. La Commission estime qu'il est évident que le délégué à la protection des données, lorsque celui ci a été désigné, conseille le responsable du traitement dans l'exécution d'une AIPD. L'article 35(2) du RGPD confirme explicitement que lorsqu'un délégué à la protection des données a été désigné, le responsable du traitement demandera conseil auprès de lui lorsqu'il effectue une AIPD.

77. La responsabilité finale d'une bonne exécution de l'AIPD incombe, tout comme pour les autres obligations prévues par le RGPD, au responsable du traitement et non au délégué à la protection des données. Le RGPD précise en effet clairement que c'est le responsable du traitement qui doit mettre en oeuvre des mesures appropriées pour assurer et être en mesure de démontrer la conformité de leurs opérations avec les dispositions du RGPD[118]. Le rôle du délégué est dès lors un rôle consultatif, pas un rôle de décision[119].

78. Comme déjà indiqué ci-dessus, la Commission estime indispensable que le responsable du traitement prenne les mesures nécessaires afin de veiller à ce que les bonnes personnes au sein de l'entreprise soient impliquées dans le processus d'évaluation des risques. Le but n'est pas que le délégué à la protection des données rédige seul l'intégralité d'une AIPD[120].

79. Le rôle consultatif du délégué à la protection des données doit notamment porter sur les éléments suivants :

- faut-il effectuer ou non une AIPD ;
- quelle méthodologie faut-il suivre lors de la réalisation d'une AIPD ;
- l'AIPD doit-elle être effectuée en interne ou être externalisée ;
- quelles garanties (dont les mesures techniques et organisationnelles) doivent être appliquées afin d'atténuer les risques éventuels pesant sur les droits et les intérêts des personnes concernées ;

[118] Groupe 29, Lignes directrices concernant les délégués à la protection des données, p. 21. Voir les articles 5(2) et 24(1) du RGPD.

[119] Toute autre interprétation pourrait en outre donner lieu à un conflit d'intérêts : voir Groupe 29, Lignes directrices concernant les délégués à la protection des données, p. 20 ("*Cela signifie en particulier que le DPD ne peut exercer au sein de l'organisme une fonction qui l'amène à déterminer les finalités et les moyens du traitement de données à caractère personnel.*").

[120] C'est ce qui ressort notamment de l'article 39(1)c, qui dispose que le délégué à la protection des données "dispense des *conseils*, sur demande, en ce qui concerne l'AIPD et *vérifie* son exécution".

- la question de savoir si l'AIPD a été correctement réalisée et si ses conclusions (opportunité ou non de procéder au traitement et garanties à mettre en place) sont conformes au RGPD[121].

Si le responsable du traitement n'est pas d'accord avec l'avis rendu par le délégué à la protection des données, il faut motiver spécifiquement et par écrit dans la documentation de l'AIPD pourquoi il n'a pas été tenu compte de cet avis[122].

D) Les personnes concernées ou leurs représentants

80. L'article 35(9) du RGPD dispose que :

"*Le cas échéant, le responsable du traitement demande l'avis des personnes concernées ou de leurs représentants au sujet du traitement prévu, sans préjudice de la protection des intérêts généraux ou commerciaux ou de la sécurité des opérations de traitement.*".

81. La Commission fait remarquer que la lecture séparée des versions anglaise, française et néerlandaise de l'article 35(9) du RGPD pourrait donner lieu à des interprétations divergentes. Là où la version néerlandaise indique que la consultation des personnes concernées ou de leurs représentants doit se faire "*in voorkomend geval*", le texte anglais indique qu'une telle consultation doit se faire "*where appropriate*". Le texte français indique quant à lui "*le cas échéant*".

82.La Commission estime que l'idée derrière la formulation choisie est univoque, plus précisément que la décision de procéder ou non à la consultation des personnes concernées (ou de leurs représentants) revient en premier lieu au responsable du traitement. Il n'est toutefois pas entièrement facultatif pour le responsable du traitement de consulter ou non les personnes concernées ou leurs représentants. Là où il existe suffisamment de motifs importants de procéder à une telle consultation, compte tenu de la nature, du contexte, de la portée et de la finalité du traitement, ainsi que de l'impact potentiel sur les personnes concernées, il est nécessaire qu'une telle consultation ait effectivement lieu. Une consultation des personnes concernées est en particulier recommandée lorsqu'elles disposent d'informations essentielles ou qu'elles peuvent formuler des remarques importantes qui sont pertinentes pour la réalisation de l'AIPD. Si le responsable du traitement juge qu'il n'est pas approprié de demander l'avis des personnes concernées, par exemple parce que cela compromettrait la confidentialité de plans d'affaires ou serait disproportionné ou irréalisable, il doit documenter sa motivation de ne pas s'enquérir de l'avis des personnes concernées[123].

---

[121] Groupe 29, Lignes directrices concernant les délégués à la protection des données, p. 20.

[122] Idem. Le Groupe 29 conseille par ailleurs que le responsable du traitement fixe clairement, par exemple dans le contrat du délégué à la protection des données, mais aussi dans les informations fournies aux travailleurs, au management (et à d''autres personnes concernées, au besoin), les tâches précises du délégué à la protection des données et leur ampleur, notamment en ce qui concerne la réalisation d'une analyse d'impact relative à la protection des données.

[123] Groupe 29, Lignes directrices AIPD, p. 18-19.

83. La consultation de personnes concernées ou de leurs représentants peut présenter une plus-value importante, tant lors de l'identification et de l'évaluation des risques du traitement que lors de la finalisation d'une AIPD, afin de vérifier si tous les risques ont été suffisamment cernés. L'ampleur de la consultation (quelles personnes ainsi que leur nombre) sera déterminée de préférence en fonction du risque et de l'ampleur du traitement. Si un traitement envisagé n'entraîne des risques que pour un nombre limité de personnes concernées (par exemple les travailleurs d'une petite organisation), la consultation peut se limiter à un nombre restreint de ces travailleurs et/ou de leurs représentants. Si le traitement envisagé implique des risques pour un grand nombre de personnes concernées (par exemple tous les habitants), il convient alors d'organiser une consultation plus large[124].

84.Le responsable du traitement décide en principe librement de la manière dont les personnes concernées ou leurs représentants sont consultés. Leur avis peut être recueilli de différentes manières, selon le contexte (par exemple une étude générique relative aux finalités et aux moyens du traitement, une question adressée aux représentants du personnel ou des enquêtes habituelles qui sont envoyées aux futurs clients du responsable du traitement)[125]. S'il dispose de leurs coordonnées, il peut les contacter directement pour leur demander leur avis au sujet du traitement de données envisagé (par exemple par e-mail). Si l'identité des personnes concernées n'est pas connue au préalable, le responsable du traitement pourrait par exemple organiser une consultation publique. Au besoin, le responsable du traitement peut aussi prévoir un moment de concertation commun. Bien que l'article 35(9) du RGPD n'évoque que les "personnes concernées ou leurs représentants", il peut aussi y avoir une plus-value à demander le point de vue d'organisations qui défendent de manière plus générale les intérêts de personnes concernées ou de consommateurs.

85. Dans le cadre de la consultation, le responsable du traitement doit veiller à ce que les questions soient posées de manière à générer des résultats fiables (par exemple au moyen d'un questionnaire validé).

86. Si la décision finale du responsable du traitement diffère de l'avis des personnes concernées, il y a lieu qu'il documente les raisons de sa décision de persévérer ou non[126].

E) L'autorité de contrôle

87. Comme cela a déjà été mentionné, une consultation préalable n'est obligatoire que s'il s'avère que le risque résiduel du traitement envisagé est élevé. Si le risque peut être limité efficacement à l'aide de mesures techniques et organisationnelles appropriées, aucune consultation préalable ne doit avoir lieu.

---

[124] ISO/IEC 29134, "Information technology – Security techniques – Guidelines for privacy impact assessment", 2017, p. 13.

[125] Groupe 29, Lignes directrices AIPD, p. 18.

[126] Groupe 29, Lignes directrices AIPD, p. 18.

88. La Commission souscrit au choix politique du législateur européen qui consiste à ne soumettre que les cas problématiques à un avis préalable. Il s'agit d'une application du "principe de responsabilité" et on souligne également que l'autorité de contrôle doit pouvoir concentrer ses activités là où le besoin se fait le plus sentir. Cela n'empêche pas que le responsable du traitement doit être prêt à soumettre, à la demande de l'autorité de contrôle, une AIPD pour tous ces traitements susceptibles d'engendrer un risque élevé pour les droits et libertés des personnes physiques.

F) Le grand public

89. Il n'y a pas d'obligation légale de publier une AIPD. C'est le responsable du traitement qui décide lui-même de publier ou non une AIPD. La Commission encourage toutefois les responsables du traitement à envisager la publication d'une AIPD[127]. L'AIPD publiée ne doit pas comporter l'intégralité de l'analyse, surtout lorsque l'AIPD pourrait contenir des informations spécifiques relatives à des risques en matière de sécurité concernant le responsable du traitement ou divulguer des secrets d'affaires ou des informations commercialement sensibles. Dans de tels cas, la version publiée peut consister simplement en un résumé des principales constatations de l'AIPD, ou même uniquement en une déclaration selon laquelle une AIPD a été effectuée[128].

8. Dispositions particulières

A) Traitement en vertu d'une obligation légale ou de l'intérêt public

90. L'article 35(10) du RGPD prévoit deux circonstances dans lesquelles l'obligation de procéder à une AIPD n'est potentiellement pas d'application, à savoir :

- lorsque le traitement envisagé est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis ; et
- lorsque le traitement envisagé est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement.

Afin que cette exception soit d'application, il faut toutefois que :

- le traitement trouve son fondement dans le droit de l'Union ou dans le droit de l'État membre auquel le responsable du traitement est soumis ;

[127] Groupe 29, Lignes directrices AIPD, p. 22. La publication peut accroître la confiance dans les opérations de traitement du responsable du traitement et donner des gages de transparence. Il est notamment de bonne pratique de publier une AIPD lorsque des citoyens sont affectés par l'opération de traitement. Tel peut en particulier être le cas lorsqu'une autorité publique réalise une AIPD. (Id.)

[128] Groupe 29, Lignes directrices AIPD, p. 22.

- le traitement spécifique ou l'ensemble des opérations de traitement en question soient régis dans ce cadre ; et
- une AIPD ait déjà été effectuée en tant qu'élément d'une analyse d'impact générale dans le cadre de l'adoption de ce fondement[129].

En outre, le législateur est toujours libre de prévoir qu'une AIPD soit toujours réalisée avant le traitement[130].

91. La Commission rappelle que l'autorité de contrôle doit en général être consultée lors de la préparation d'une mesure législative ou réglementaire qui concerne la protection des données à caractère personnel[131]. L'existence ou non d'une consultation préalable ne doit toutefois pas porter préjudice à l'obligation générale du responsable du traitement de réaliser une gestion des risques, conformément à l'article 24(1) du RGPD. De plus, la Commission estime que la réalisation d'une AIPD (complémentaire) dans certains cas peut toujours être opportune ou nécessaire, en particulier lorsque lors de la préparation d'une mesure législative ou réglementaire, on n'a aucune notion claire des traitements de données qui auront lieu dans le cadre de l'exécution[132].

B) Opérations de traitement similaires ou conjointes

92. Une AIPD peut porter sur un seul traitement de données ou sur une série de traitements similaires[133]. Une seule AIPD peut suffire pour plusieurs traitements qui sont similaires en termes de nature, portée, contexte, finalité et risques. Une AIPD vise en effet à assurer l'étude systématique des nouvelles situations susceptibles d'entraîner des risques élevés pour les droits et libertés des personnes physiques, et il n'est pas nécessaire de procéder à une AIPD dans les cas (à savoir des opérations de traitement effectuées dans un contexte spécifique et à des fins spécifiques) qui ont déjà été étudiés. Tel peut être le cas lorsque des technologies similaires sont utilisées pour collecter le même type de données pour les mêmes finalités[134].

---

[129] Le considérant (93) du RGPD apporte un peu plus de lumière sur cette disposition : "*Au moment de l'adoption de la législation nationale régissant les missions de l'autorité publique ou de l'organisme public concernés ainsi que l'opération ou l'ensemble d'opérations de traitement en question, les États membres peuvent estimer qu'une telle analyse est nécessaire préalablement au traitement*."

[130] Article 35(10) du RGPD *in fine*.

[131] Voir l'article 57(1)c du RGPD.

[132] Voir aussi Groupe 29, Lignes directrices AIPD, p. 15 ("*Dans le cas d'une AIPD réalisée au stade de l'élaboration de la législation conférant une base juridique au traitement, un réexamen pourra être nécessaire avant le lancement des opérations, la législation adoptée étant susceptible de différer de la proposition d'une manière affectant les questions liées à la protection de la vie privée et à la protection des données. En outre, il est possible que les détails techniques disponibles en ce qui concerne le traitement effectif soient insuffisants au moment de l'adoption de la législation, même si une AIPD a été effectuée. Dans de tels cas, il pourra s'avérer nécessaire d'effectuer une AIPD spécifique avant d'exécuter les activités de traitement proprement dites.*")

[133] Article 35(1) du RGPD. Voir aussi Groupe 29, Lignes directrices AIPD, p. 8.

[134] Article 35(1) du RGPD. Voir aussi Groupe 29, Lignes directrices AIPD, p. 8. Par exemple, un groupe d'autorités municipales mettant chacune en place un système similaire de surveillance par CCTV pourrait se contenter d'une AIPD unique couvrant le traitement envisagé par chacun de ces responsables distincts; un opérateur ferroviaire (un seul responsable du traitement) pourrait quant à lui couvrir la vidéosurveillance de l'ensemble de ses gares au moyen d'une seule et même AIPD. (*Id.*)

93. Dans certains cas, il peut être raisonnable et utile d'élargir la portée de l'AIPD au-delà d'un projet unique, par exemple lorsque des autorités publiques ou organismes publics entendent mettre en place une application ou une plateforme de traitement commune, ou lorsque plusieurs responsables du traitement envisagent de créer une application ou un environnement de traitement communs à tout un secteur ou segment professionnel, ou pour une activité transversale largement utilisée[135]. La Commission encourage les responsables du traitement qui ont l'intention de créer une application ou une plateforme de traitement commune à réaliser une AIPD sur une base commune (dans les cas où une AIPD est requise)[136]. La même recommandation s'applique également aux responsables du traitement qui, en raison de leurs activités, font partie d'une organisation ou association de coordination (comme par exemple des écoles, clubs sportifs, mouvements de jeunesse, médecins, avocats, journalistes, etc.) lorsque chacun de ces responsables du traitement envisage une série de traitements similaires impliquant des risques élevés similaires.

C) Codes de conduite

94. L'article 35(8) du RGPD dispose que:

> "*Le respect, par les responsables du traitement ou sous-traitants concernés, de codes de conduite approuvés visés à l'article 40 est dûment pris en compte lors de l'évaluation de l'impact des opérations de traitement effectuées par lesdits responsables du traitement ou sous-traitants, en particulier aux fins d'une analyse d'impact relative à la protection des données.*"

95. L'article 40 du RGPD dispose que "*les États membres, les autorités de contrôle, le comité et la Commission encouragent l'élaboration de codes de conduite destinés à contribuer à la bonne application du présent règlement, compte tenu de la spécificité des différents secteurs de traitement et des besoins spécifiques des micro, petites et moyennes entreprises*. Conformément à l'article 35(8) du RGPD, le responsable du traitement doit prendre en considération de tels codes de conduite lorsqu'une AIPD est réalisée. La Commission attire enfin encore l'attention sur le fait que la Commission européenne peut, au moyen d'un acte d'exécution, rendre obligatoires certains codes de conduite, après approbation de ceux-ci par le CEPD[137].

D) Gestion et contrôle

96. L'article 35(11) du RGPD dispose que le responsable du traitement doit, si nécessaire, procéder à un examen afin d'évaluer si le traitement est effectué conformément à l'AIPD. Un tel examen doit au

[135] Considérant (92) du RGPD.

[136] À cet égard, voir la section 3 ci-avant.

[137] Article 40(9) du RGPD.

moins avoir lieu quand il se produit une modification du risque présenté par les opérations de traitement[138].

97. L'article 35(11) du RGPD comporte deux éléments : d'une part une obligation de vérifier au besoin si le traitement de données est bien effectué conformément à l'AIPD (incluant les mesures de protection indiquées) et d'autre part l'obligation de revoir l'AIPD quand il se produit une modification du risque.

98. Une modification du risque présenté par l'opération de traitement peut être due à différents éléments, comme une modification des moyens de traitement employés ou une évolution dans l'état des connaissances (par exemple lorsque de nouvelles techniques de minimalisation de données sont disponibles) ou la découverte d'une nouvelle vulnérabilité dans la sécurité justifiant la prise de mesures de sécurité supplémentaires ou nouvelles[139]. La révision d'une AIPD peut également s'avérer nécessaire s'il y a une modification du contexte organisationnel ou social de l'opération de traitement (par exemple s'il s'avère que les effets de certaines décisions automatisées se sont accrus ou que de nouvelles catégories de personnes concernées apparaissent vulnérables à la discrimination). Dans chacun de ces exemples, le facteur en cause peut entraîner une évolution des risques découlant de l'activité de traitement concernée[140].

99. Inversement, certaines évolutions peuvent aussi réduire les risques. Prenons par exemple le cas d'une opération de traitement ayant évolué de telle sorte que les prises de décisions ne sont plus automatisées ou celui d'une activité de surveillance ayant perdu son caractère systématique. Dans ce cas, le réexamen des risques peut montrer qu'une AIPD n'est plus nécessaire[141].

100. Étant donné que les risques évoluent généralement avec le temps, la Commission recommande de prévoir expressément une vérification périodique lors de la réalisation d'une AIPD[142]. La fréquence de la vérification périodique doit être déterminée en fonction du risque présenté par l'opération de traitement. En outre, la réalisation d'une AIPD peut elle-même révéler des facteurs requérant un suivi particulier (par exemple des mesures techniques et organisationnelles dont l'efficacité n'est pas encore établie). Dans le cadre d'une bonne gestion des risques, la Commission s'attend à ce que le responsable du traitement effectue un contrôle au moins tous les 3 ans. La Commission recommande également que le résultat du contrôle soit officiellement soumis à

---

[138] Article 35(11) du RGPD.

[139] Voir aussi F. Bieker, M. Friedwald, M. Hansen, H. Obersteller et M. Rost, "A Process for Data Protection Impact Assessment Under the European General Data Protection Regulation", in S. Schiffner et al. (Eds.), APF (Annual Privacy Forum) 2016, 2016, p. 24.

[140] Groupe 29, Lignes directrices AIPD, p. 17.

[141] Groupe 29, Lignes directrices AIPD, p. 16-17.

[142] Voir plus haut, le point 61.

l'approbation des membres de la direction de l'organisation du responsable du traitement ou à un organe interne mandaté[143].

E) Quid des traitements déjà existants ?

101. L'obligation de réaliser une AIPD s'applique à partir du 25 mai 2018. Les traitements susceptibles de donner lieu à un risque élevé et qui commencent après le 25 mai 2018 devront dès lors être précédés d'une AIPD. Pour les traitements déjà existants, une AIPD n'est en principe requise que si les risques pour les droits et libertés des personnes physiques changent après le 25 mai 2018, par exemple parce qu'une nouvelle technologie est employée ou parce que les données à caractère personnel sont utilisées pour une autre finalité[144].

102. Les éléments qui précèdent ne signifient pas que les responsables du traitement ne doivent réaliser une AIPD que lorsque le traitement lui-même est adapté. Comme indiqué plus haut, les risques présentés par une opération de traitement peuvent aussi évoluer en raison de changements de l'environnement dans lequel le traitement de données a lieu (par exemple le contexte social, les conséquences du traitement), pouvant faire apparaître de nouvelles vulnérabilités[145]. Dès qu'il est question d'une modification du risque présenté par l'opération de traitement (et que le traitement est toujours susceptible d'engendrer un risque élevé), la réalisation d'une AIPD est obligatoire.

103. La Commission recommande quoi qu'il en soit au responsable du traitement, à titre de bonne pratique, de procéder à la réalisation d'une AIPD pour tous les traitements existants qui sont susceptibles d'engendrer un risque élevé pour les droits et libertés des personnes physiques. Même si une AIPD n'est pas requise au sens strict au 25 mai 2018, il est nécessaire que le responsable du traitement réalise une AIPD au bon moment dans le cadre de sa responsabilité générale et de la gestion des risques[146].

104. Les traitements qui ont déjà fait l'objet d'une autorisation (générale ou spécifique) par un des comités sectoriels de la Commission ne doivent en principe pas faire l'objet d'une AIPD pour autant que le traitement soit réalisé conformément aux modalités préalables de l'autorisation. Le considérant (171) du RGPD dispose en effet que les autorisations qui ont été accordées par les autorités de contrôle sur le fondement de la directive 95/46/CE demeurent en vigueur jusqu'à ce qu'elles soient modifiées, remplacées ou abrogées[147]. À l'inverse, ceci signifie que tout traitement de données dont les conditions de mise en oeuvre (portée, finalités, données à caractère personnel collectées, identité des

[143] Voir plus haut, le point 71.

[144] Groupe 29, Lignes directrices AIPD, p. 16-17.

[145] Voir plus haut, le point 98.

[146] Groupe 29, Lignes directrices AIPD, p. 17.

[147] Voir également à cet égard l'article 111 de la loi du 3 décembre 2017 *portant création de l'Autorité de protection des données*.

responsables du traitement ou des destinataires des données, durée de conservation des données, mesures techniques et organisationnelles, etc.) ont changé depuis l'autorisation et sont susceptibles d'engendrer un risque élevé doit faire l'objet d'une AIPD[148].

F) Amende possible en cas de non-respect

105. Si on ne répond pas aux exigences des articles 35 et 36 du RGPD, cela peut entraîner une amende. Le fait de ne pas effectuer d'AIPD alors que le traitement est soumis à l'obligation d'une telle analyse (article 35 du RGPD, paragraphes 1, 3 et 4), de réaliser l'analyse d'une manière incorrecte (article 35 du RGPD, paragraphes 2 et 7 à 9) ou de ne pas consulter l'autorité de contrôle compétente lorsque la situation l'exige (article 36 du RGPD, paragraphe 3, point e), est passible d'une amende administrative pouvant s'élever jusqu'à 10.000.000 EUR ou, dans le cas d'une entreprise, jusqu'à 2 % du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu[149].

L'Administrateur f.f., Le Président,

(sé) An Machtens (sé) Willem Debeuckelaere

[148] Groupe 29, Lignes directrices AIPD, p. 16. Comme indiqué plus haut, en vertu de l'article 35(10) du RGPD, l'obligation de réaliser une AIPD ne s'appliquera pas dans certaines conditions lorsque le traitement envisagé est nécessaire pour répondre à une obligation légale incombant au responsable du traitement ou lorsque le traitement envisagé est nécessaire pour accomplir une tâche d'intérêt général dans le cadre de l'exercice de l'autorité publique qui incombe au responsable du traitement. Voir plus haut, les points 90-91.

[149] Groupe 29, Lignes directrices AIPD, p. 5.

9. Annexe 1 : Caractéristiques minimales d'une bonne gestion des risques

Tout responsable du traitement choisit lui-même quelle procédure et quelle méthode il souhaite utiliser pour évaluer et gérer les risques, à condition qu'elles répondent à un certain nombre de caractéristiques minimales de fiabilité et d'objectivité[150]. Afin d'éviter qu'une situation d'insécurité juridique ne survienne, à défaut d'éléments complémentaires permettant de contrôler la qualité d'une analyse des risques, la Commission formule ci-après plusieurs **caractéristiques minimales**. La Commission souligne qu'il s'agit ici de caractéristiques minimales qui, en soi, ne comportent aucune garantie que le(s) traitement(s) visé(s) aura (auront) lieu conformément au RGPD.

1. Étayée méthodologiquement

La gestion des risques et l'appréciation des risques doivent être étayées méthodologiquement, de préférence à l'aide de méthodes déjà existantes en matière de gestion des risques. L'utilisation de normes internationales, telles que celles développées par l'Organisation internationale de normalisation (ISO)[151], ainsi que de codes de conduite élaborés ou agréés au niveau européen, est particulièrement importante dans ce cadre. Le responsable du traitement peut toutefois choisir librement quelle méthode il souhaite utiliser, à condition que celle-ci permette une évaluation objective du risque et tienne compte des éléments minimaux prescrits par le RGPD. Le responsable du traitement doit cependant indiquer explicitement quelle méthode a été choisie et doit veiller à ce qu'elle soit appliquée de manière cohérente.

2. Structurée

Une bonne gestion des risques se déroule de manière structurée, où l'on peut généralement distinguer les étapes suivantes[152] :

- communication et consultation avec des parties intéressées internes et externes ;
- définition du contexte pertinent (incluant une description de l'objet de l'analyse de risque, une définition des critères servant à évaluer les risques pour les droits et libertés des personnes physiques et la définition de valeurs de risques (in)acceptables) ;
- identification, analyse et évaluation des risques (y compris l'identification des vulnérabilités, des menaces et l'attribution d'une valeur de risque) ;

---

[150] Voir plus haut, le point 51. Il est important que la méthode choisie permette d'analyser les risques du point de vue de la personne concernée. Étant donné qu'une AIPD est un instrument servant à gérer les risques pour les droits des personnes concernées, la perspective de la personne concernée est centrale. Cette situation est différente de la gestion de risques dans d'autres domaines (comme par exemple la sécurité de l'information), qui est généralement axée sur les intérêts et les finalités de l'organisation elle-même.

[151] Voir en particulier la norme ISO 31000 (Risk management) et la norme ISO 27005 (Information security risk management). Ces normes ont une portée générale et ne sont pas spécifiquement dédiées à la réalisation d'une AIPD. En les appliquant, il convient de tenir compte de l'interprétation particulière que le RGPD confère à la notion de "risque", ainsi que des garanties potentielles et des mécanismes qui peuvent être activés pour limiter ces risques.

[152] Basé sur IEC/ISO, "Risk management – Risk management techniques", IEC/ISO 31010, v1.0, 2009-11, p. 8.

- identification de mesures d'atténuation des risques appropriées (c'est-à-dire les mesures techniques, organisationnelles et juridiques qui sont nécessaires pour ramener le risque à un niveau acceptable) ; et
- gestion et contrôle.

3. Sur mesure

Une évaluation des risques est toujours un travail sur mesure et est adaptée au contexte et au profil de risque de l'entreprise qui réalise l'évaluation[153]. Une bonne appréciation du risque ne consiste pas à reproduire simplement des analyses réalisées précédemment mais exige une évaluation concrète sur la base du contexte spécifique (c'est-à-dire en référence à la nature, au champ d'application, au contexte et aux finalités du traitement). Rien n'empêche par contre qu'un responsable du traitement utilise des procédures ou des modèles élaborés par (ou en collaboration avec) d'autres entités (par exemple au niveau d'un secteur ou d'une branche d'activités déterminé(e)) pour réaliser une évaluation des risques.

4. Compréhensible

Le résultat d'une appréciation des risques doit être lisible et accessible à un public aussi large que possible. Le résultat ne peut pas être seulement lisible pour des experts (en risques), des techniciens ou du personnel spécialisé. Des résumés succincts et des représentations visuelles (par exemple des graphiques en couleur, des tableaux avec des chiffres) peuvent favoriser l'accessibilité de l'analyse des risques (tant son processus que sa transcription)[154].

5. Suffisamment nuancée

Une analyse des risques doit comporter suffisamment d'échelles afin de permettre une évaluation nuancée des risques identifiés. Ne prévoir que trois échelles (bas, moyen, élevé) pour apprécier les risques n'est pas toujours suffisant pour donner lieu à une appréciation correcte. Une description claire des critères utilisés pour évaluer le risque est quoi qu'il en soit indispensable.

6. Communication et consultation

Un bon système de gestion des risques implique ceux qui sont les mieux placés pour contribuer au processus d'identification, d'analyse, d'évaluation et de gestion des risques. Ce groupe comprend non seulement le délégué à la protection des données et/ou le conseiller en sécurité mais également les concepteurs de nouvelles applications, ceux qui prennent des décisions stratégiques en matière de développement de projets et les membres du personnel (ou leurs représentants) qui utiliseront les

---

[153] IEC/ISO, " Management du risque – Principes et lignes directrices", ISO 31000, v1.0, 2009-11, p. 8.

[154] La Commission comprend que la documentation qui est générée au cours du processus d'appréciation du risque puisse présenter un niveau supérieur de technicité qui peut ne pas être immédiatement accessible aux personnes qui ne sont pas des experts. Elle souligne seulement que le résultat de l'appréciation du risque doit toujours être lisible et accessible.

données à caractère personnel en question dans le cadre de l'exercice de leurs missions. Le cas échéant, le responsable du traitement demande l'avis des personnes concernées ou de leurs représentants, sans préjudice de la protection des intérêts généraux ou commerciaux ou de la sécurité des opérations de traitement.

7. Gestion et contrôle

Un rapport daté et écrit des appréciations du risque effectuées doit être rédigé. Un organe interne mandaté qui prend des décisions (par exemple le comité de direction, le comité stratégique ou le comité de sécurité, mandaté par le conseil de direction) doit être informé périodiquement du résultat (ou du statut) du processus d'appréciation du risque. Cet organe mandaté doit approuver formellement l'évaluation des risques ainsi que les mesures visant à atténuer les risques.

Le processus d'appréciation du risque ne peut toutefois pas être réduit à un simple processus bureaucratique. Le responsable du traitement doit prendre des mesures adéquates afin de veiller à ce que la bonne gestion des risques fasse partie de la "culture d'entreprise" du responsable du traitement.

Une appréciation du risque qui a été effectuée doit être contrôlée périodiquement et au moins en cas de circonstances changeantes pouvant avoir une influence essentielle sur une appréciation qui a été réalisée dans le passé. La fréquence de la vérification périodique doit être déterminée en fonction du risque présenté par l'opération de traitement. En outre, la Commission recommande également que le résultat du contrôle soit officiellement soumis à l'approbation de la plus haute autorité au sein de l'organisation du responsable du traitement.

10. Annexe 2 : Projet de liste des types d'opérations de traitement pour lesquelles une AIPD est requise (art. 35(4) du RGPD)

L'article 35(4) du RGPD oblige chaque autorité de contrôle à établir une liste des types d'opérations de traitement pour lesquelles une AIPD est requise et à communiquer ensuite cette liste au Comité européen de la protection des données (CEPD). Lorsque cette liste comprend des activités de traitement liées à l'offre de biens ou de services à des personnes concernées ou au suivi de leur comportement dans plusieurs États membres, ou peuvent affecter sensiblement la libre circulation des données à caractère personnel au sein de l'Union, il faut appliquer préalablement à l'établissement de la liste le mécanisme de contrôle visé à l'article 63[155].

La Commission souligne que l'existence d'une liste des opérations de traitement pour lesquelles une AIPD est requise ne porte en rien préjudice à l'obligation générale du responsable du traitement de procéder à une bonne appréciation du risque et à une bonne gestion des risques. La réalisation d'une AIPD ne dispense d'ailleurs aucunement le responsable du traitement de l'obligation de respecter les autres obligations du RGPD ou d'autres obligations imposées par la législation générale ou spécifique au secteur. En outre, la liste ci-dessous n'est absolument pas exhaustive : une AIPD est toujours requise dès que les conditions d'application définies à l'article 35(1) du RGPD sont remplies[156]. Enfin, la Commission attire encore l'attention sur le fait que ces listes sont évolutives et peuvent être adaptées s'il s'avère qu'elles n'atteignent pas leur objectif.

La compétence de dresser une liste des types de traitements pour lesquels une AIPD est obligatoire au sens de l'article 35(4) du RGPD n'incombe pas à la Commission mais à l'Autorité de protection des données, l'instance qui succédera de plein droit à la Commission à partir du 25 mai 2018. Dès lors, la liste ci-après ne sera juridiquement contraignante que si elle est arrêtée par l'Autorité de protection des données, le cas échéant après application du mécanisme de contrôle de la cohérence visé à l'article 63 du RGPD.

Outre les cas prévus à l'article 35(3) du RGPD et compte tenu de l'exception prévue par l'article 35(10) du RGPD, une AIPD sera toujours requise :

[155] Article 35(6) du RGPD.

[156] La simple circonstance qu'un traitement de données envisagé ne corresponde pas avec un des types de traitement repris dans la liste (par exemple parce qu'une des caractéristiques n'est pas présente) ne signifie donc pas qu'il y aurait pour ce traitement une dispense de l'obligation de réaliser une AIPD conformément à l'article 35(1) du RGPD.

1. lorsque le traitement utilise des données biométriques en vue de l'identification unique des personnes concernées[157] se trouvant dans un lieu public ou dans un lieu privé accessible au public ;

2. lorsque des données à caractère personnel sont collectées auprès de tiers afin d'être prises ensuite en considération dans le cadre de la décision de refuser ou de cesser un contrat de service déterminé avec une personne physique ;

3. lorsque le traitement concerne des catégories particulières de données à caractère personnel au sens de l'article 9 du RGPD qui sont (ré)utilisées pour une (des) finalité(s) autre(s) que celle(s) pour laquelle (lesquelles) elles ont été collectées, sauf lorsque le traitement se fonde sur le consentement de la personne concernée ou s'il est nécessaire pour répondre à une obligation légale à laquelle le responsable du traitement est soumis[158] ;

4. lorsque le traitement est réalisé à l'aide d'un implant et qu'une violation de données à caractère personnel[159] pourrait compromettre la santé physique de la personne concernée ;

5. en cas de traitement à grande échelle de données à caractère personnel de personnes physiques vulnérables, notamment les enfants, pour une (des) finalité(s) autre(s) que celle(s) pour laquelle (lesquelles) elles ont été collectées ;

6. lorsque des données sont collectées à grande échelle auprès de tiers afin d'analyser ou de prédire la situation économique, la santé, les préférences ou centres d'intérêt personnels, la fiabilité ou le comportement, la localisation ou les déplacements de personnes physiques ;

7. lorsque des catégories particulières de données à caractère personnel au sens de l'article 9 du RGPD ou des données de nature très personnelle (comme des données sur la pauvreté, le chômage, l'implication de l'aide à la jeunesse ou le travail social, des données sur les activités domestiques et privées, des données de localisation) sont échangées systématiquement entre plusieurs responsables du traitement ;

8. lorsqu'il est question d'un traitement à grande échelle de données générées au moyen d'appareils dotés de capteurs qui envoient des données via Internet ou via un autre moyen (applications de "l'Internet des objets", comme les télévisions intelligentes, les appareils ménagers intelligents, les jouets connectés, les smart cities, les compteurs d'énergie intelligents, etc.) et que ce traitement sert à analyser ou prédire la situation économique, la santé, les préférences ou centres d'intérêt

---

[157] L'article 4(14) du RGPD définit les "données biométriques" comme étant les données à caractère personnel résultant d'un traitement technique spécifique, relatives aux caractéristiques physiques, physiologiques ou comportementales d'une personne physique, qui permettent ou confirment son identification unique, telles que des images faciales ou des données dactyloscopiques.

[158] Il s'agit ci d'un traitement de catégories particulières de données pour une finalité autre que celle pour laquelle les données ont été collectées et qui n'est pas fondé sur le consentement de la personne concernée ou sur le droit de l'Union ou le droit d'un État membre, tel que visé par l'article 6(4) du RGPD.

[159] L'article 4(12) du RGPD définit une "violation de données à caractère personnel" comme une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données.

personnels, la fiabilité ou le comportement, la localisation ou les déplacements de personnes physiques ;

9. lorsqu'il est question d'un traitement à grande échelle et/ou systématique de données de téléphonie, d'Internet ou d'autres données de communication, de métadonnées ou de données de localisation de personnes physiques ou permettant de mener à des personnes physiques (par exemple le wifi-tracking ou le traitement de données de localisation de voyageurs dans les transports publics) lorsque le traitement n'est pas strictement nécessaire pour un service demandé par la personne concernée ;

10. lorsqu'il est question de traitements de données à caractère personnel à grande échelle où le comportement[160] de personnes physiques est observé, collecté, établi ou influencé, y compris à des fins publicitaires, et ce de manière systématique via un traitement automatisé.

Le responsable du traitement qui envisage un des types de traitements précités est obligé de réaliser une AIPD avant de procéder au traitement. Cela ne signifie toutefois pas nécessairement qu'une consultation préalable doit également avoir lieu. Si le risque peut être suffisamment limité à l'aide de mesures techniques et organisationnelles appropriées, aucune consultation préalable n'est requise.

[160] Par exemple le comportement de visionnage, d'écoute, de navigation, de clic, physique ou d'achat.

11. Annexe 3 : Projet de liste des types d'opérations de traitement pour lesquelles aucune AIPD n'est requise (art. 35(5) du RGPD)

L'article 35(5) du RGPD autorise l'autorité de contrôle à établir une liste des types d'opérations de traitement pour lesquelles une AIPD n'est pas requise.

La Commission souhaite souligner que la liste susmentionnée ne porte en rien préjudice à l'obligation générale du responsable du traitement de procéder à une bonne appréciation du risque et à une bonne gestion des risques, conformément à l'article 24(1) du RGPD[161]. Cette obligation générale d'appréciation du risque et de gestion des risques s'applique sans préjudice de l'existence d'une liste de traitements spéciaux pour lesquels une AIPD n'est pas requise en tant que telle. Enfin, la Commission attire encore l'attention sur le fait que ces listes sont évolutives et peuvent être adaptées s'il s'avère qu'elles n'atteignent pas leur objectif.

Pour les types de traitement suivants, une AIPD n'est pas requise :

1. les traitements réalisés par des entités privées qui sont nécessaires pour répondre à une *obligation légale* qui leur incombe, moyennant une définition par la loi des finalités du traitement, des catégories de données à caractère personnel traitées et des garanties destinées à prévenir les abus ou l'accès ou le transfert illicites ;
2. les traitements de données à caractère personnel qui concernent uniquement des données qui sont nécessaires à *l'administration des salaires* de personnes en service ou actives pour le compte du responsable du traitement lorsque les données sont exclusivement utilisées pour cette administration des salaires, sont uniquement communiquées aux destinataires qui sont autorisés à cet effet et ne sont pas conservées plus longtemps que le temps nécessaire aux finalités du traitement ;
3. les traitements de données à caractère personnel qui concernent exclusivement *l'administration du personnel* en service ou actif pour le compte du responsable du traitement, dans la mesure où ce traitement ne porte pas sur des données relatives à la santé de la personne concernée, ni sur des catégories particulières de données au sens de l'article 9 du RGPD, ni sur des condamnations pénales et des infractions au sens de l'article 10 du RGPD ou sur des données ayant pour but une évaluation de la personne concernée et où les données à caractère personnel traitées ne sont pas conservées plus longtemps que le temps nécessaire à l'administration du personnel et uniquement dans le cadre de l'application d'une disposition légale ou réglementaire ou sont communiquées si nécessaire à des tiers pour la réalisation des finalités du traitement ;

[161] Voir plus haut, le point 10.

4. les traitements de données à caractère personnel qui concernent exclusivement *la comptabilité* du responsable du traitement lorsque les données sont exclusivement utilisées pour cette comptabilité, lorsque le traitement concerne uniquement les personnes dont les données sont nécessaires pour la comptabilité et lorsque les données à caractère personnel ne sont pas conservées plus longtemps que nécessaire à la réalisation des finalités du traitement et que les données à caractère personnel traitées sont uniquement communiquées à des tiers dans le cadre de l'application d'une disposition légale ou réglementaire ou lorsque la communication est nécessaire pour la comptabilité ;

5. les traitements de données à caractère personnel qui concernent exclusivement *l'administration des actionnaires et associés* lorsque le traitement porte uniquement sur des données nécessaires à cette administration, lorsque ces données concernent uniquement des personnes dont les données sont nécessaires à cette administration, lorsque les données sont communiquées à des tiers uniquement dans le cadre de l'application d'une disposition légale ou réglementaire et que les données à caractère personnel ne sont pas conservées plus longtemps que le temps nécessaire à la réalisation des finalités du traitement ;

6. les traitements de données à caractère personnel effectués par une *fondation, association ou toute autre institution sans but lucratif* dans le cadre de ses activités habituelles, pour autant que le traitement porte uniquement sur des données à caractère personnel relatives à ses propres membres, relatives aux personnes avec lesquelles le responsable du traitement entretient des contacts réguliers et relatives aux bénéficiaires de la fondation, association ou institution et qu'aucune personne ne soit enregistrée sur la base de données obtenues de tiers et que les données à caractère personnel traitées ne soient pas conservées plus longtemps que le temps nécessaire à l'administration des membres, des personnes de contact et des bénéficiaires et soient uniquement communiquées à des tiers dans le cadre de l'application d'une disposition légale ou réglementaire ;

7. les traitements de données à caractère personnel qui concernent exclusivement *l'enregistrement de visiteurs* dans le cadre d'un contrôle d'accès lorsque les données traitées restent limitées au nom et à l'adresse professionnelle du visiteur, à l'identification de son employeur, à l'identification du véhicule du visiteur, au nom, à la section et à la fonction de la personne visitée et au moment de la visite et où les données à caractère personnel traitées peuvent exclusivement être utilisées pour le contrôle d'accès et ne pas être conservées plus longtemps que le temps nécessaire à cette finalité ;

8. les traitements de données à caractère personnel effectués par *des établissements d'enseignement* en vue de la gestion de leurs relations avec leurs élèves ou étudiants dans le cadre de leurs missions d'enseignement, dans la mesure où le traitement ne porte que sur des données à caractère personnel relatives à des élèves ou étudiants potentiels, actuels et anciens de l'établissement d'enseignement en question et qu'aucune personne ne soit enregistrée sur la base de données obtenues de tiers et que ces données soient uniquement communiquées à des tiers dans le cadre de l'application d'une disposition légale ou réglementaire et ne soient pas conservées plus longtemps que le temps nécessaire à la gestion de la relation avec l'élève ou l'étudiant ;
9. les traitements de données à caractère personnel qui concernent exclusivement la *gestion de la clientèle ou des fournisseurs* du responsable du traitement, pour autant que le traitement concerne uniquement des clients ou fournisseurs existants et anciens du responsable du traitement et que le traitement ne concerne pas des catégories particulières de données au sens de l'article 9 du RGPD, ni des condamnations pénales et des infractions visées à l'article 10 du RGPD et qu'en ce qui concerne l'administration de la clientèle, aucune donnée provenant de tiers soit enregistrée et que les données à caractère personnel traitées ne soient pas conservées pour une durée excédant celle nécessaire à la gestion normale de l'entreprise du responsable du traitement et ces données ne peuvent être transmises à des tiers que dans le cadre de l'application d'une disposition légale ou réglementaire ou pour la gestion normale de l'entreprise.