Projet de recommandation d'initiative concernant l'analyse d'impact relative à la protection des données et la consultation préalable soumis à la consultation publique (CO-AR-2016-004)

À partir du 25 mai 2018, le Règlement général sur la protection des données (RGPD) sera d'application. Le RGPD confirme des principes de protection des données déjà existants mais prévoit également plusieurs nouveaux droits et nouvelles obligations. Depuis quelque temps, la Commission de la protection de la vie privée reçoit de plus en plus de questions concernant la portée exacte de ces nouveaux droits et nouvelles obligations.

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". Une AIPD est un processus visant à évaluer les risques liés aux droits et libertés de personnes physiques qui surviennent ou menacent de survenir dans le cadre du traitement de données à caractère personnel, et à évaluer les possibilités de gestion de ces risques. La nouvelle obligation d'exécuter une AIPD soulève d'emblée plusieurs questions pratiques, comme : quand une AIPD est-elle obligatoire ? Quels sont les éléments requis d'une AIPD ? Quels acteurs doivent être impliqués dans une AIPD ?

Avant d'émettre une recommandation d'initiative sur ce thème, la Commission souhaite recueillir l'avis et les suggestions des divers acteurs concernés : responsables du traitement, sous-traitants et personnes concernées. En outre, la Commission s'attend à ce que le Groupe 29[1] et l'ENISA[2] promulguent à relativement court terme des directives complémentaires sur la méthode d'exécution d'une AIPD en vertu du RGPD. Là où la Commission l'estime opportun, ces directives complémentaires seront intégrées dans la version finale de la recommandation.

La présente consultation, publiée le 20 décembre 2016, sera clôturée le 28 février 2017. La Commission prendra ensuite toutes les remarques en considération lors de l'élaboration de sa recommandation d'initiative.

Tous les avis, remarques ou autres propositions sont adressés à la Commission vie privée par courrier (Rue de la Presse, 35 à 1000 Bruxelles) ou par e-mail (commission@privacycommission.be).

[1] Voir les priorités définies par le Groupe 29 dans sa déclaration du 2 février 2016, publiée sur http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2016/wp236_en.pdf.

[2] Voir l'annonce de l'ENISA de janvier 2016 concernant (notamment) l'aspect de l'appréciation des risques du RGPD sur ce point https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/enisa2019s-position-on-the-general-data-protection-regulation-gdpr/.

Projet de recommandation n° [numéro/]/[année]
du [date]

Objet : projet de recommandation d'initiative concernant l'analyse d'impact relative à la protection des données et la consultation préalable (CO-AR-2016-004)

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 les articles 35 et 36 du 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)* ;

Vu le rapport de Willem Debeuckelaere ;

Émet, le 2016, la recommandation suivante :

Table des matières

1. Introduction

1. Le Règlement général relatif à la protection des données ("RGPD")[3] est entré en vigueur le 24 mai 2016. Le RGPD sera d'application à partir du 25 mai 2018.[4]

2. Le RGPD prévoit plusieurs nouvelles obligations pour le responsable du traitement[5], dont l'obligation de procéder, dans certains cas, à une analyse d'impact relative à la protection des données ("AIPD"). Une AIPD est un processus visant à évaluer les risques liés aux droits et libertés des personnes physiques qui surviennent ou menacent de survenir dans le cadre du traitement de données à caractère personnel, et à évaluer les possibilités de gestion de ces risques[6].

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

(1) les éléments essentiels d'une AIPD (point 3) ;
(2) les circonstances dans lesquelles une AIPD est obligatoire (point 4) ;
(3) les circonstances dans lesquelles une consultation préalable est obligatoire (point 5) ;
(4) les acteurs qui doivent être impliqués dans une AIPD (point 6) ; et
(5) plusieurs dispositions particulières (point 7).

4. Avant d'aborder les aspects susmentionnés, il est utile d'expliquer le contexte juridique de l'obligation de procéder à une AIPD, afin de favoriser une bonne compréhension de la *ratio legis*.

2. Contexte juridique : la responsabilité et l'approche fondée sur les risques

5. L'obligation de procéder 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.

6. 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

---

[3] Règlement (UE) 2016/79 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)*, J.O. 4 mai 2016, L 119/1.

[4] Article 99(2) du RGPD.

[5] 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.

[6] 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) : "*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 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.*"

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.

7. Le principe de la responsabilité du responsable du traitement va de pair avec une approche fondée sur les risques (ce qu'on appelle une "***risk-based approach***")[8]"). L'article 24(1) du RGPD dispose que "*Compte tenu de la nature, de la portée, du contexte et des finalités du traitement ainsi que des* ***risques***, *dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques, le responsable du traitement doit prendre des mesures techniques et organisationnelles appropriées pour s'assurer (...) que le traitement est effectué conformément au présent règlement*".

8. L'approche fondée sur les risques du RGPD a pour but de promouvoir une "**approche évolutive et proportionnelle**"[9] sans remettre en question les principes de protection des données ou les droits des personnes concernées[10]. Cela signifie qu'il faudra prendre davantage de mesures de protection pour des traitements à risque élevé que pour des traitements à risque faible.

9. 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[11]. 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.

---

[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] En anglais : "*a scalable and proportionate approach to compliance*". (Ibid., p. 2).

[10] 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.)

[11] Considérant (89) du RGPD.

3. Éléments essentiels d'une AIPD telle que requise par l'article 35 du RGPD

A) Aperçu

10. 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) Inventaire des opérations de traitement envisagées et des finalités du traitement

11. 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. Dans ce cadre, il importe qu'aussi bien les opérations de traitement que les finalités visées soient décrites de manière complète, cohérente et claire. Lors de la description des opérations de traitement, la Commission s'attend à ce que le responsable du traitement tienne compte de l'obligation de tenir un registre des activités de traitement reprise à l'article 30 du RGPD. Outre une description des finalités du traitement, cette disposition prévoit également que le responsable du traitement conserve notamment les informations suivantes :

- une description des catégories de personnes concernées et des catégories de données à caractère personnel ;
- les catégories de destinataires auxquels les données à caractère personnel ont été ou seront communiquées, y compris les destinataires dans des pays tiers ou des organisations internationales ;
- le cas échéant, les transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale, y compris l'identification de ce pays tiers ou de cette organisation internationale et, dans le cas des transferts visés à l'article 49, paragraphe 1, deuxième alinéa, les documents attestant de l'existence de garanties appropriées ;

- dans la mesure du possible, les délais prévus pour l'effacement des différentes catégories de données.

Le responsable du traitement doit veiller à ce que les opérations de traitement et finalités du traitement visées soient décrites avec la précision nécessaire. Il faut éviter un renvoi à des finalités générales, décrites au sens large (comme par ex. "améliorer l'expérience d'utilisateur", "sécurité IT", "analyse")[12]. 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.

C) Contrôle de la proportionnalité

12. Une AIPD doit évaluer la nécessité et la proportionnalité des opérations de traitement au regard des finalités. Le responsable du traitement doit dès lors indiquer 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 la (les) finalité(s) poursuivie(s). Si plusieurs traitements ou moyens du traitement peuvent être utilisés pour atteindre la (les) finalité(s) visée(s), la Commission s'attend à ce que le responsable du traitement indique explicitement pour quelle(s) raison(s) les moyens du traitement choisis sont moins intrusifs que les alternatives.

13. Lors de l'analyse de la proportionnalité, le responsable du traitement doit également examiner l'efficacité du traitement envisagé (peut-on raisonnablement espérer que le traitement envisagé atteindra sa finalité (légitime) ?). Enfin, le responsable du traitement doit aussi veiller à maintenir un équilibre adéquat entre les intérêts pertinents[13].

D) Évaluation des risques

- *La notion de "risque"*

14. La notion de "risque" peut être interprétée de plusieurs façons. Dans la littérature, on décrit généralement la notion de "risque" comme la **possibilité** ("probabilité") qu'une menace déterminée se présente, avec pour conséquence un **impact** déterminé ("gravité")[14].

[12] Voir également l'Article 29 Data Protection Working Party, "Opinion 03/2013 on purpose limitation", 2 avril 2013, p. 15-16.

[13] 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 25-26).

[14] Voir par ex. I. Naumann (ed.), "Privacy and Security Risks when Authenticating on the Internet with European eID Cards", ENISA, 26 novembre 2009. Voir également ISO, "Management du risque – Vocabulaire", 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*").

- *La notion d' "appréciation du risque"*[15]

15. La notion d' "appréciation du risque" au sens de ISO Guide 73:2009 renvoie à *l'ensemble du processus d'identification des risques (1), d'analyse du risque (2) et d'évaluation du risque* (3)[16]. L'**identification** des risques renvoie au *processus de recherche, de reconnaissance et de description des risques*[17]. L'**analyse** du risque renvoie au *processus mis en œuvre pour comprendre la nature d'un risque et pour déterminer le niveau de risque*[18]. L'**évaluation** du risque est le *processus de comparaison des résultats de l'analyse du risque avec les critères de risque afin de déterminer si le risque et/ou son importance sont acceptables ou tolérables*[19].

16. 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 se produise lorsqu'aucune mesure de protection n'est prise. 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)[20].

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

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*. Selon le Groupe 29, les termes "*pour les droits et libertés des personnes physiques*" dans le RGPD[21] concernent principalement le droit au respect de la vie privée mais ils peuvent également se rapporter à d'autres droits et libertés fondamentaux, comme la liberté d'expression, la liberté de pensée, de conscience et de religion, l'interdiction de discrimination et le droit à la liberté de mouvement[22].

18. Plusieurs traitements de données peuvent comporter plusieurs risques (inhérents) pour les droits et libertés des personnes physiques. Le considérant (75) du RGPD énumère, à titre d'exemple, un certain nombre de circonstances dans lesquelles les traitements engendrent des risques pour les droits et libertés des personnes physiques, à savoir :

---

[15] Au sens de la norme ISO, "Management du risque – Vocabulaire", ISO Guide 73:2009.

[16] ISO, "Management du risque – Vocabulaire", ISO Guide 73:2009.

[17] Id.

[18] Id.

[19] Id.

[20] Voir également ISO, "Management du risqué – Vocabulaire", ISO Guide 73:2009 qui définit le "*risque résiduel*" comme "*risque subsistant après le traitement du risque*".

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

[22] Article 29 Data Protection Working Party, "Statement on the role of a risk-based approach in data protection legal frameworks", WP218, 30 mai 2014, p. 4.

- lorsque le traitement peut donner lieu à une discrimination, à un vol ou une usurpation d'identité, à une perte financière, à une atteinte à la réputation, à une perte de confidentialité de données protégées par le secret professionnel, à un renversement non autorisé du processus de pseudonymisation ou à tout autre dommage économique ou social important ;
- lorsque les personnes concernées pourraient être privées de leurs droits et libertés ou empêchées d'exercer le contrôle sur leurs données à caractère personnel ;
- lorsque le traitement concerne des données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, la religion ou les convictions philosophiques, l'appartenance syndicale, ainsi que des données génétiques, des données concernant la santé ou des données concernant la vie sexuelle ou des données relatives à des condamnations pénales et à des infractions, ou encore à des mesures de sûreté connexes ;
- lorsque des aspects personnels sont évalués, notamment dans le cadre de l'analyse ou de la prédiction d'éléments concernant le rendement au travail, la situation économique, la santé, les préférences ou centres d'intérêt personnels, la fiabilité ou le comportement, la localisation ou les déplacements, en vue de créer ou d'utiliser des profils individuels ;
- lorsque le traitement porte sur des données à caractère personnel relatives à des personnes physiques vulnérables, en particulier les enfants ; ou
- lorsque le traitement porte sur un volume important de données à caractère personnel et touche un nombre important de personnes concernées.

- *Besoin d'une analyse contextuelle*

19. La Commission souligne qu'une appréciation du risque doit toujours se faire en fonction de l'ensemble des circonstances particulières de chaque traitement (ou groupe d'opérations de traitement similaires[23]). 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 la vie privée et pour les droits et libertés des personnes et doit prendre les mesures adéquates pour garantir l'application des dispositions du règlement.

[23] Conformément à l'article 35(1) du RGPD, une AIPD peut porter sur un ensemble d'opérations de traitement similaires qui présentent des risques élevés similaires (voir ci-après le point 33).

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

20. En règle générale, le responsable du traitement est libre de choisir la méthodologie qu'il souhaite utiliser, à condition que celle-ci réponde à un certain nombre de caractéristiques minimales de confidentialité et d'objectivité[24] et tienne compte des éléments minimaux prescrits par le RGPD. Il appartient au responsable du traitement d'utiliser une méthodologie qui lui permet de respecter les exigences du RGPD.

21. La Commission estime en outre important que chaque responsable du traitement qui entreprend une AIPD utilise une méthodologie qui soit adaptée aux besoins et au contexte de sa propre entreprise.

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

23. En outre, la Commission recommande vivement que le responsable du traitement se base sur des méthodologies déjà existantes en matière de gestion des risques. L'utilisation de normes internationales, telles que celles développées par l'Organisation internationale de normalisation (ISO)[25], ainsi que de codes de conduite élaborés ou agréés au niveau européen, est particulièrement importante dans ce cadre[26].

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

E) Mesures visées

25. Une AIPD ne comprend pas uniquement une appréciation des risques mais aussi les 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 présent règlement a été respecté. Ce n'est qu'après la prise en considération des mesures de protection visées que l'on peut évaluer le risque résiduel du traitement envisagé.

---

[24] 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.*"

[25] En particulier la norme ISO 31000 (Risk management) et la norme ISO 27005 (Information security risk management).

[26] Voir également ENISA, "ENISA Position on the Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications of March 31, 2010", juillet 2010, p. 6, qui peut être consultée via le lien https://www.enisa.europa.eu/media/news-items/enisa-opinion-on-pia. En ce qui concerne les codes de conduite agréés ou élaborés au niveau européen, voir également ci-après les points 60 et suivants.

26. 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[27].

4. Circonstances dans lesquelles une AIPD est obligatoire

27. 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 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[28]. 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 offrent aux contrôleurs nationaux la possibilité d'établir des listes des types d'opérations de traitement pour lesquelles une AIPD est requise ou non.

A) Notion de "susceptible d'engendrer un risque élevé" pour les droits et libertés des personnes physiques

28. 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 traitement effectue, avant le traitement, une analyse de l'impact des opérations de traitement envisagées sur la protection des données à caractère personnel. Une seule et même analyse peut porter sur un ensemble d'opérations de traitement similaires qui présentent des risques élevés similaires.*"

29. La notion de "susceptible d'engendrer un 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 méthodologies 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 méthodologie utilisées. La notion de "susceptible d'engendrer un risque élevé" au sens du RGPD ne correspond toutefois pas nécessairement à la notion de "susceptible d'engendrer un risque élevé" telle qu'on la retrouve dans d'autres modèles de gestion des risques.

---

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

[28] Article 35(1) du RGPD.

30. La Commission estime que la notion de "susceptible d'engendrer un risque élevé" renvoie tout d'abord aux traitements de données dont il est *vraisemblable* qu'ils puissent avoir des *conséquences néfastes considérables* pour les libertés et droits fondamentaux des personnes physiques si l'on ne prévoit pas de mesures de protection adéquates. Une "conséquence considérable" signifie que, dans le cas où le risque se produirait, la personne concernée serait sensiblement touchée dans l'exercice ou la jouissance de ses libertés et droits fondamentaux. C'est par exemple le cas lorsqu'il est vraisemblable que le traitement puisse engendrer les conséquences néfastes qui sont énumérées au considérant (75) du RGPD[29].

31. Contrairement à l'article 36 du RGPD, l'élément "susceptible d'engendrer un risque élevé" qui donne lieu à l'obligation de procéder à une AIPD concerne le risque "inhérent" du traitement de données envisagé. Le "risque résiduel" n'intervient que dans le cadre de l'application de l'obligation de procéder à une consultation préalable de l'autorité de contrôle (voir ci-dessous aux points 40 et suivants)[30].

B) Situations définies à l'article 35(3) du RGPD

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

a) en cas d'*évaluation systématique et exhaustive des aspects personnels de l'individu* reposant sur du profilage et sur la base de laquelle seront prises des décisions de nature à produire des effets juridiques en ce qui concerne les personnes concernées ou à les impacter de manière importante ;

b) en cas de *traitement à grande échelle de catégories particulières de données* 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*[31].

Dans ces cas-là, il faudra toujours faire une AIPD préalable. 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 encore un avocat. Dans de tels cas, le traitement ne peut être considéré comme effectué à grande échelle.

---

[29] Voir ci-dessus, le point 18.

[30] En ce qui concerne la distinction entre les risques "inhérents" et les risques "résiduels", voir ci-dessus le point 16.

[31] Pour l'interprétation des notions en NL de "systematisch", "stelselmatig" et "grootschalig" et en FR de "systématique" et de "à grande échelle", la Commission renvoie aux directives du Groupe 29 relatives au délégué à la protection des données (Article 29 Data Protection Working Party, "Guidelines on Data Protection Officers", WP 243, 13 décembre 2016, p. 7-8). 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".

33. Il existe des cas dans lesquels 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[32]. 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). La même recommandation s'applique également aux responsables du traitement qui, dans le chef de leurs activités, font partie d'une organisation ou d'une association de coordination (comme par ex. les écoles, clubs sportifs, mouvements de jeunesse, médecins, avocats, journalistes, ...) lorsque chacun de ces responsables du traitement vise toute une série de traitements similaires qui impliquent des risques élevés similaires.

C) Les listes de l'autorité de contrôle

34. 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.

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

36. La Commission souhaite insister sur le fait que les listes susmentionnées ne portent aucunement préjudice à l'obligation générale du responsable du traitement de toujours prévoir, en vertu de l'article 24(1) du RGPD, des mesures techniques et organisationnelles appropriées pour garantir que le traitement est exécuté conformément au présent règlement, compte tenu notamment des risques pour les droits et libertés des personnes physiques. 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 est requise (ou de l'existence d'une liste des opérations de traitement pour lesquelles une AIPD n'est pas requise).

[32] Considérant (92) du RGPD.

37. De plus, les listes ne sont nullement exhaustives : une AIPD est toujours requise dès que les conditions d'application définies à l'article 35 du RGPD sont remplies.

38. 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.

39. 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.

5. Circonstances dans lesquelles une consultation préalable est obligatoire

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

> *"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."*

41. Il ressort clairement de la formulation de l'article 36(1) du RGPD qu'une consultation préalable n'est obligatoire que lorsque le risque résiduel est élevé. Ce n'est que lorsqu'il s'avère que le traitement envisagé présenterait un risque élevé si le responsable du traitement ne prenait pas de mesures efficaces d'atténuation des risques que le traitement doit préalablement être soumis à l'autorité de contrôle. Si le risque peut être limité efficacement à l'aide de mesures techniques et organisationnelles appropriées, aucune consultation préalable ne doit avoir lieu[33].

42. Si l'autorité de contrôle est d'avis que le traitement envisagé n'est pas conforme au règlement ou que les risques ne sont pas suffisamment identifiés ou atténués, elle fournit par écrit, 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. Ce délai de 8 semaines peut être prolongé de six semaines[34]. 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).

---

[33] La Commission souligne que la notion de "mesures organisationnelles" ne renvoie pas uniquement à la communication et à la hiérarchie au sein d'une entreprise. Les procédures et directives à l'attention du personnel sont également essentielles à cet égard.

[34] 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.

43. 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 présent règlement ;

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 ; et

f) toute autre information que l'autorité de contrôle demande.

6. Les acteurs concernés

A) Le responsable du traitement

44. 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 obligatoire en vertu de l'article 35 du RGPD.

45.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'appréciation du risque. Afin d'éviter que le processus d'appréciation du risque soit ramené à un pur exercice écrit, ceux qui sont les mieux placés pour contribuer à une appréciation du risque 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 également aux concepteurs de nouvelles applications, à ceux qui prennent des décisions stratégiques en matière de développement de projets et aux membres du personnel (ou à leurs représentants) qui utiliseront les données à caractère personnel en question dans le cadre de l'exercice de leurs missions.

46. En outre, la Commission recommande également que la plus haute autorité au sein de l'organisation du responsable du traitement soit suffisamment impliquée dans le processus d'appréciation du risque. L'appréciation du risque (avec ou sans AIPD), l'approbation d'une AIPD ou la décision de ne pas procéder à une AIPD serait par exemple officiellement soumise à l'aval des membres de la direction.

B) Le sous-traitant

47. 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 stipulé 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*"[35].

48. Le considérant (95) confirme en outre 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.

49. À la lumière des dispositions susmentionnées, l'autorité de contrôle tiendra compte, dans le cadre de l'évaluation de l'obligation d'assistance du sous-traitant, de (1) la nature du traitement ; (2) des informations mises à disposition du sous-traitant ; (3) de l'opportunité de l'aide du sous-traitant afin de parvenir à une apppréciation et à une gestion des risques correctes et de qualité.

C) Le délégué à la protection des données

50. La Commission estime qu'il est évident que le délégué à la protection des données, lorsque celui-ci a été désigné, assiste le responsable du traitement et le conseille 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.

51. 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'appréciation du risque. La Commission juge dès lors qu'il n'est pas souhaitable que le délégué à la protection des données rédige seul une AIPD, sans la contribution des acteurs pertinents.

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

D) Les personnes concernées ou leurs représentants

52. 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.*".

53. La Commission fait remarquer que la lecture séparée des versions anglaise, française et néerlandaise de l'article 35(9) 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*".

54.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. Sa décision est toutefois soumise à un contrôle marginal de l'autorité de contrôle, vu son pouvoir général d'application des règles. En d'autres termes, la consultation des personnes concernées ou de leurs représentants n'est pas entièrement facultative pour le responsable du traitement. 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, la Commission estime nécessaire qu'une telle consultation ait effectivement lieu.

E) L'autorité de contrôle

55. 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.

56. 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.

57. La Commission estime que les explications contenues dans la présente recommandation ainsi que les directives édictées au niveau européen (en particulier par le Groupe de travail Article 29 et l'ENISA)

et les normes internationales pertinentes offrent une assise très solide au responsable du traitement pour réaliser correctement une gestion des risques.

7. Dispositions particulières

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

58. 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 ;
- 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[36].

En outre, le législateur est toujours libre de déterminer qu'une AIPD doit toujours être réalisée avant le traitement[37].

59. 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[38]. 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.

---

[36] Le considérant (93) 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*".

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

[38] Voir l'articles 57(1)c du RGPD.

B) Codes de conduite

60. 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.*"

61.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[39].

C) Contrôle

62. Le responsable du traitement est tenu de vérifier, si nécessaire, si le traitement est effectué conformément à l'AIPD. Un tel contrôle doit au moins avoir lieu lorsqu'il est question d'un changement du risque qu'impliquent les traitements[40].

63. Vu la constatation selon laquelle les risques évoluent généralement avec le temps, la Commission estime opportun que le responsable du traitement inclue lui-même un contrôle périodique de l'AIPD réalisée. 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 2 ans. La Commission recommande également que le résultat du contrôle soit officiellement soumis à l'approbation des membres de la direction ou des cadres de l'organisation du responsable du traitement[41].

64.Enfin, la Commission attire l'attention sur le fait qu'il existe aussi d'autres circonstances pouvant donner lieu à la révision d'une AIPD réalisée précédemment, comme une modification des moyens de traitement utilisés ou une évolution de l'état de la technique (par ex. lorsque de nouvelles techniques de minimisation des données sont disponibles) ou la découverte d'une nouvelle vulnérabilité dans la

[39] Article 40(9) du RGPD.

[40] Article 35(11) du RGPD.

[41] Voir également ci-dessus le point 46.

sécurité qui justifient l'adoption de nouvelles mesures de sécurité ou de mesures de sécurité complémentaires[42].

L'Administrateur f.f., Le Président,

An Machtens Willem Debeuckelaere

[42] Voir également 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.

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

En règle générale, le responsable du traitement est libre d'utiliser la procédure et la méthodologie qu'il souhaite lors de l'appréciation et de la gestion des risques, à condition que celle-ci réponde à un certain nombre de caractéristiques minimales de fiabilité et d'objectivité[43].

Afin d'éviter qu'une situation d'insécurité juridique ne survienne, à défaut d'éléments objectifs permettant de contrôler la qualité d'une méthodologie déterminée, la Commission formule ci-après plusieurs **caractéristiques minimales**. Ces éléments ne sont pas neufs mais étaient déjà documentés ailleurs[44]. 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 méthodologies déjà existantes en matière de gestion des risques. L'utilisation de normes internationales, telles que celles développées par l'Organisation internationale de normalisation (ISO)[45], ainsi que de codes de conduite élaborés ou agréés au niveau européen, est particulièrement importante dans ce cadre[46].

Le responsable du traitement doit explicitement indiquer quelle méthodologie a été choisie et doit veiller à ce que celle-ci soit appliquée de manière cohérente tout au long du processus de l'AIPD.

2. Structurée

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

---

[43] Le considérant (76) du RGPD confirme le caractère objectif de cette appréciation du risque à l'égard du traitement et des conséquences de celui-ci pour les droits et libertés des personnes : "*Il convient de déterminer la probabilité et la gravité du risque pour les droits et libertés de la personne concernée en fonction de la nature, de la portée, du contexte et des finalités du traitement. 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.*"

[44] Voir ISACA, "Privacy Audit - Methodology and Related Considerations, *Isaca Journal* 2014 ; Volume 1, qui peut être consulté via http://www.isaca.org/Journal/archives/2014/Volume-1/Documents/Privacy-Audit-Methodology-and-Related-Considerations_joa_Eng_0114.pdf, ENISA, "ENISA Position on the Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications of March 31, 2010", juillet 2010, p. 6-9, qui peut être consultée via https://www.enisa.europa.eu/media/news-items/enisa-opinion-on-pia et OCDE, "Digital Security Risk Management for Economic and Social Prosperity", OECD Recommendation and Companion Document, 2015, qui peut être consultée sur http://www.oecd.org/sti/ieconomy/digital-security-risk-management.pdf.

[45] En particulier la norme ISO 31000 (Risk management) et la norme ISO 27005 (Information security risk management).

[46] Voir également ENISA, "ENISA Position on the Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications of March 31, 2010", juillet 2010, p. 6.

- définition du contexte pertinent (constitué des paramètres externes et internes qui doivent être pris en considération dans le cadre de la gestion des risques) ;
- définition des critères d'évaluation des risques pour les droits et libertés des personnes physiques ;
- identification et analyse des risques (y compris l'identification des vulnérabilités, des menaces et l'attribution d'une valeur de risque) ;
- définition de valeurs de risque acceptables (y compris une détermination des valeurs de risques qui ne sont pas acceptables) ; et
- identification de mesures d'atténuation des risques appropriées (c'est-à-dire les mesures techniques et organisationnelles qui sont nécessaires pour ramener le risque à un niveau acceptable).

3. Sur mesure

Une appréciation du risque est toujours sur mesure. 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 qui ont été élaborés par (ou conjointement avec) d'autres entités (par ex. au niveau d'un secteur ou d'une branche d'activité déterminés) lors de l'exécution de l'appréciation du risque.

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 ex. des graphiques en couleur, des tableaux avec des chiffres) peuvent favoriser l'accessibilité de l'appréciation des risques (tant son processus que sa transcription)[47].

5. Suffisamment nuancée

Une appréciation du risque doit comporter suffisamment d'échelles afin de permettre une évaluation nuancée des risques identifiés[48]. Ne prévoir que trois échelles (bas, moyen, élevé) pour apprécier les risques est généralement insuffisant pour donner lieu à une appréciation correcte.

---

[47] 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.

[48] Voir par exemple ISACA, privacy Audit-Methodology and Related Considerations, Isaca Journal, Volume 1, 2014, http://www.isaca.org/Journal/archives/2014/Volume-1/Documents/Privacy-Audit-Methodology-and-Related-Considerations_joa_Eng_0114.pdf.

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. La Commission pense ici en premier lieu non seulement au délégué à la protection des données et/ou au conseiller en sécurité mais également aux concepteurs de nouvelles applications, à ceux qui prennent des décisions stratégiques en matière de développement de projets et aux membres du personnel (ou à leurs représentants) qui utiliseront les données à caractère personnel en question dans le cadre de l'exercice de leurs missions.

7. Gestion et contrôle

Un rapport daté et écrit des appréciations du risque effectuées doit être rédigé. Un organe mandaté interne qui prend les décisions (par ex. 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. 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 2 ans. 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.

9. Annexe 2 : 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).

La Commission souhaite souligner que l'existence d'une liste de traitements particuliers pour lesquels 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. En outre, la liste ci-dessous n'est nullement exhaustive : une AIPD est toujours requises dès que les conditions d'application définies à l'article 35 du RGPD sont remplies. 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.

Outre les cas prévus à l'article 35(2) du RGPD et compte tenu de l'exception prévue par l'article 35(10), une AIPD sera toujours requise :

1. lorsque le traitement utilise la biométrie afin d'identifier les personnes concernées ;
2. lorsque le traitement utilise des données génétiques ;
3. 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 le service ;
4. lorsque le traitement sert à évaluer la solvabilité financière de la personne concernée ou à générer tout autre profil de risque de la personne concernée qui est pris en considération dans le service à la personne concernée (ou dans le cadre de la décision de refuser ou de cesser un service) ;
5. lorsque le traitement est de nature à ce qu'une violation des données à caractère personnel puisse compromettre la santé physique de la personne concernée ;
6. lorsque le traitement concerne des données à caractère personnel financières ou sensibles 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 est soit basé sur le consentement de la personne concernée, soit nécessaire pour remplir une obligation légale qui incombe au responsable du traitement ;
7. lorsque le traitement donne lieu à une communication ou à une mise à disposition du public de données à caractère personnel relatives à un grand nombre de personnes concernées ;

8. lorsque des aspects personnels sont évalués pour notamment analyser ou prévoir des prestations professionnelles, une situation économique, la santé, des préférences ou intérêts personnels, la fiabilité ou le comportement, la localisation ou les déplacements ;
9. lorsque des profils de personnes physiques sont établis à grande échelle ;
10. en cas de traitement à grande échelle de données à caractère personnel de personnes physiques vulnérables, à savoir les enfants, pour une (des) finalité(s) autre(s) que celle(s) pour laquelle (lesquelles) elles ont été collectées ;
11. 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 et pour lesquels des données sensibles sont utilisées ;
12. lorsque le traitement vise à enregistrer les connaissances, les prestations, les aptitudes ou l'état de santé mentale d'élèves et à assurer le suivi de l'évolution de ceux-ci, notamment à l'aide de systèmes de suivi des élèves, que ces élèves soient dans l'enseignement primaire, secondaire, tertiaire ou universitaire.

10. Annexe 3 : 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. 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 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 ;
2. 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 données sensibles ou judiciaires au sens des articles 9 et 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 ;
3. 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 ;

4. 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 ;

5. 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 ;

6. 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 ;

7. 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.