GROUPE DE TRAVAIL «ARTICLE 29» SUR LA PROTECTION DES DONNÉES

17/FR

WP 248 rév. 01

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

Adoptées le 4 avril 2017

Telles que modifiées et adoptées en dernier lieu le 4 octobre 2017

LE GROUPE DE TRAVAIL SUR LA PROTECTION DES PERSONNES À L'ÉGARD DU TRAITEMENT DES DONNÉES À CARACTÈRE PERSONNEL

institué en vertu de la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995,

vu les articles 29 et 30 de ladite directive,

vu son règlement intérieur,

A ARRÊTÉ LES PRÉSENTES LIGNES DIRECTRICES:

SOMMAIRE

I. Introduction

Le règlement (UE) 2016/679[1] (RGPD) s'appliquera à partir du 25 mai 2018. De la même manière que la directive 2016/680[2], l'article 35 du RGPD introduit la notion d'analyse d'impact relative à la protection des données (AIPD[3]),

Une AIPD est un processus dont l'objet est de décrire le traitement, d'en évaluer la nécessité ainsi que la proportionnalité et d'aider à gérer les risques pour les droits et libertés des personnes physiques liés au traitement de leurs données à caractère personnel[4], en les évaluant et en déterminant les mesures nécessaires pour y faire face. Les AIPD sont un outil important au regard du principe de responsabilité, compte tenu de leur utilité pour les responsables du traitement non seulement aux fins du respect des exigences du RGPD, mais également en ce qui concerne leur capacité à démontrer que des mesures appropriées ont été prises pour assurer la conformité au règlement (voir également l'article 24)[5]. Autrement dit, **une AIPD est un processus qui vise à assurer la conformité aux règles et à pouvoir en apporter la preuve**.

---

[1] 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).

[2] L'article 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 dispose également qu'une analyse d'impact sur la vie privée est nécessaire lorsque le traitement «*est susceptible d'engendrer un risque élevé pour les droits et les libertés des personnes physiques*».

[3] On parle souvent, dans d'autres contextes, d'«analyse d'impact sur la vie privée» pour désigner la même notion.

[4] Si le RGPD ne définit pas formellement la notion d'AIPD en tant que telle,

- l'article 35, paragraphe 7, dispose que l'analyse doit au moins contenir:
  - «*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»;*
- son sens et son rôle sont clarifiés au considérant 84 comme suit: «*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».*

[5] Voir également le considérant 84: «*Il convient de tenir compte du résultat de cette analyse pour déterminer les mesures appropriées à prendre afin de démontrer que le traitement des données à caractère personnel respecte le présent règlement*».

En vertu du RGPD, le non-respect des exigences applicables en matière d'AIPD peut donner lieu à des amendes imposées par l'autorité de contrôle compétente. Le fait de ne pas effectuer d'AIPD alors que le traitement est soumis à l'obligation d'une telle analyse (article 35, paragraphes 1, 3 et 4), de réaliser l'analyse d'une manière incorrecte (article 35, paragraphes 2 et 7 à 9) ou de ne pas consulter l'autorité de contrôle compétente lorsque la situation l'exige (article 36, 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.

II. Objectifs des présentes lignes directrices

Les présentes lignes directrices tiennent compte:

- de la déclaration 14/EN WP 218 du groupe de travail «Article 29» sur la protection des données (GT29)[6];
- des lignes directrices 16/EN WP 243 du GT29 relatives aux délégués à la protection des données[7];
- de l'avis 13/EN WP 203 du GT29 relatif à la limitation des finalités[8];
- des normes internationales pertinentes[9].

Conformément à l'approche par les risques préconisée par le RGPD, il n'est pas obligatoire d'effectuer une AIPD pour chaque opération de traitement. Une AIPD n'est requise que lorsque le traitement est «*susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques*» (article 35, paragraphe 1). Afin de garantir une interprétation cohérente des situations dans lesquelles une AIPD est obligatoire (article 35, paragraphe 3), les présentes lignes directrices s'appliquent en premier lieu à éclaircir cet aspect et fournissent des critères pour les listes que les autorités de protection des données (APD) sont tenues d'adopter en vertu de l'article 35, paragraphe 4.

Conformément à l'article 70, paragraphe 1, point e), le Comité européen de la protection des données (CEPD) pourra publier des lignes directrices, recommandations et bonnes pratiques afin d'encourager une application cohérente du RGPD. Le présent document ayant pour objet d'anticiper les travaux futurs du CEPD, il s'emploie à clarifier les dispositions pertinentes du RGPD afin de faciliter le

[6] Déclaration 14/EN WP 218 du G29 concernant le rôle d'une approche par les risques dans les cadres juridiques de la protection des données (en anglais), adoptée le 30 mai 2014.
http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf?wb48617274=72C54532

[7] Lignes directrices 16/EN WP 243 du G29 relatives aux délégués à la protection des données (en anglais), adoptées le 13 décembre 2016.
http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_en_40855.pdf?wb48617274=CD63BD9A

[8] Avis 13/EN WP 203 du G29 de mars 2013 relatif à la limitation des finalités, adopté le 2 avril 2013.
http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf?wb48617274=39E0E409

[9] Par ex., ISO 31000:2009, *Management du risque – Principes et lignes directrices*, Organisation internationale de normalisation (ISO); ISO/IEC 29134 (projet, indisponible en français), *Technologies de l'information – Techniques de sécurité – Lignes directrices pour l'évaluation d'impacts sur la vie privée*, Organisation internationale de normalisation (ISO).

respect de la législation par les responsables du traitement et de procurer une sécurité juridique aux responsables du traitement tenus d'effectuer une AIPD.

Ces lignes directrices s'efforcent également de promouvoir la mise en place:

- d'une liste commune à l'échelle de l'Union des opérations de traitement pour lesquelles une AIPD est obligatoire (article 35, paragraphe 4);
- d'une liste commune à l'échelle de l'Union des opérations de traitement pour lesquelles une AIPD n'est pas nécessaire (article 35, paragraphe 5);
- de critères communs concernant la méthodologie à suivre pour la réalisation d'une AIPD (article 35, paragraphe 5);
- de critères communs pour la détermination des cas dans lesquels l'autorité de contrôle doit être consultée (article 36, paragraphe 1);
- de recommandations basées sur l'expérience acquise dans les États membres de l'UE, dans la mesure du possible.

III. Les AIPD: explication du règlement

Le RGPD exige des responsables du traitement qu'ils mettent en œuvre des mesures appropriées pour assurer et être en mesure de démontrer la conformité de leurs opérations avec les dispositions du règlement, en tenant compte notamment «des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques» (article 24, paragraphe 1). 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[10] que présente le traitement de données personnelles.

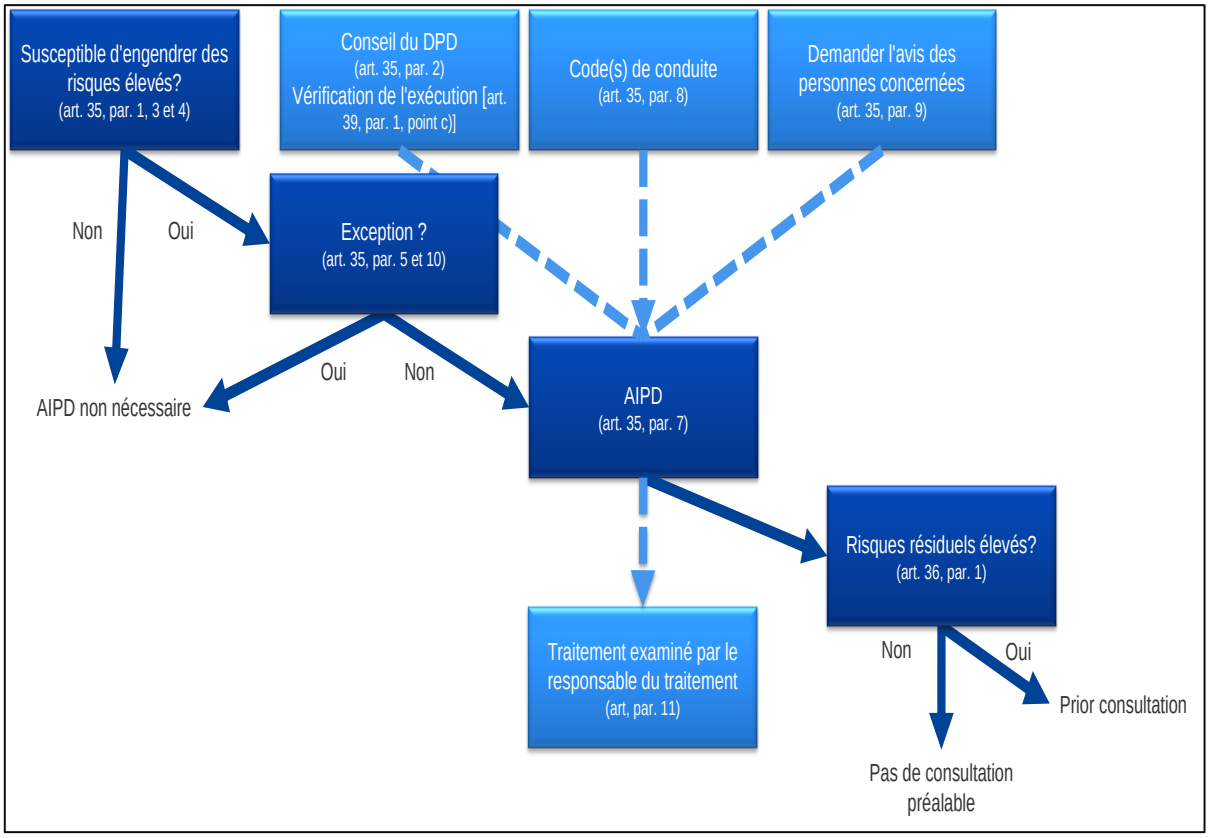
Un «risque» est un scénario qui décrit un événement et ses effets, estimés en termes de gravité et de probabilité. La «gestion du risque» peut, quant à elle, se définir comme un ensemble d'activités coordonnées dans le but de diriger et de piloter un organisme vis-à-vis du risque.

L'article 35 évoque un risque potentiellement élevé «pour les droits et libertés des personnes physiques». Comme indiqué dans la déclaration du GT29 concernant le rôle d'une approche par les risques dans les cadres juridiques de la protection des données, la référence aux «droits et libertés» des personnes concernées vise principalement les droits à la protection des données et à la vie privée, mais s'entend également, le cas échéant, pour d'autres droits fondamentaux, tels que la liberté de parole, la liberté de pensée, la liberté de circulation, l'interdiction de toute discrimination, le droit à la liberté ainsi que la liberté de conscience et de religion.

Conformément à l'approche par les risques préconisée par le RGPD, il n'est pas obligatoire d'effectuer une AIPD pour chaque opération de traitement. Ainsi, une AIPD n'est requise que lorsqu'un type de traitement est «susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques» (article 35, paragraphe 1). 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 œuvre des mesures pour gérer de manière appropriée les risques pour les droits et libertés des personnes concernées. Concrètement, cela signifie que les responsables du traitement sont tenus d'évaluer de manière continue les risques créés par leurs activités de traitement dans le but d'identifier quand un type de traitement est «susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques».

[10] Il convient de souligner que la gestion des risques pour les droits et libertés des personnes physiques suppose d'identifier ces risques, de les analyser, de les estimer, de les évaluer, de les traiter (par ex. en les atténuant) et de les réexaminer régulièrement. Les responsables du traitement ne sauraient se soustraire à leurs responsabilités en recourant à des polices d'assurance pour couvrir les risques.

Le schéma suivant illustre les principes de base adoptés par le RGPD en ce qui concerne les AIPD:



A. Sur quoi porte une AIPD? Une opération de traitement unique? Un ensemble d'opérations de traitement similaires?

Une AIPD peut concerner une opération de traitement de données unique. Cependant, l'article 35, paragraphe 1 dispose qu'«*une seule et même analyse peut porter sur un ensemble d'opérations de traitement similaires qui présentent des risques élevés similaires*». Le considérant 92 ajoute qu'«*il existe des cas dans lesquels il peut être raisonnable et économique d'élargir la portée de l'analyse d'impact relative à la protection des données 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*».

Une seule et même AIPD peut être utilisée pour évaluer plusieurs opérations de traitement similaires en termes de nature, de portée, de contexte, de finalités et de risques. En effet, les AIPD visent 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. 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. Ceci

peut également valoir pour des opérations de traitement similaires mises en œuvre par différents responsables du traitement. Dans pareils cas, il y a lieu qu'une AIPD de référence soit partagée ou rendue publiquement accessible, les mesures décrites dans l'AIPD doivent être mises en œuvre et une justification de la réalisation d'une AIPD unique doit être fournie.

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 ex.) et à ne pas divulguer de vulnérabilités.

Une AIPD peut également être utile pour évaluer l'impact sur la protection des données d'un produit technologique, par exemple un matériel ou un logiciel, lorsque celui-ci est susceptible d'être utilisé par divers responsables du traitement pour réaliser différentes opérations de traitement. Bien entendu, le responsable du traitement déployant le produit reste tenu d'effectuer sa propre AIPD pour ce qui concerne sa mise en œuvre spécifique, mais il peut s'appuyer pour cela sur une AIPD élaborée par le fournisseur du produit, le cas échéant. Prenons l'exemple de la relation entre fabricants de compteurs intelligents et entreprises de services publics. Il conviendrait que chaque fournisseur ou sous-traitant partage les informations utiles en s'assurant de ne compromettre aucun secret ni de menacer la sécurité en divulguant des vulnérabilités.

B. Quelles sont les opérations de traitement qui requièrent une AIPD? Sauf cas exceptionnel, toutes celles qui sont «*susceptibles d'engendrer un risque élevé*».

Cette section explique dans quels cas une AIPD est obligatoire et dans quels cas elle n'est pas nécessaire.

À moins que l'opération de traitement ne relève d'un cas exceptionnel [III, B, a)], il convient d'effectuer une AIPD dès lors que le traitement est «*susceptible d'engendrer un risque élevé*» [III, B, b)].

a) Quand une AIPD est-elle obligatoire? Lorsque le traitement est «*susceptible d'engendrer un risque élevé*».

Le RGPD n'exige pas une AIPD pour toute opération de traitement qui pourrait engendrer des risques pour les droits et libertés des personnes physiques. La réalisation d'une AIPD n'est obligatoire que quand le traitement est *«susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques»* (article 35, paragraphe 1, illustré par l'article 35, paragraphe 3, et complété par l'article 35, paragraphe 4). Elle est particulièrement pertinente en cas de recours à une nouvelle technologie de traitement[11].

En cas de doute quant à la nécessité d'effectuer une AIPD, dans la mesure où les AIPD sont un outil important pour les responsables du traitement aux fins du respect de la législation sur la protection des données, le GT29 recommande d'en effectuer une malgré tout.

[11] Les considérants 89 et 91 ainsi que l'article 35, paragraphes 1 et 3, fournissent d'autres d'exemples.

Même si une AIPD peut également être requise dans d'autres situations, l'article 35, paragraphe 3, considère que le traitement est *«susceptible d'engendrer un risque élevé»* en particulier dans les cas suivants:

- *«a) l'évaluation systématique et approfondie d'aspects personnels concernant des personnes physiques, qui est fondée sur un traitement automatisé, y compris le profilage, et sur la base de laquelle sont prises des décisions produisant des effets juridiques à l'égard d'une personne physique ou l'affectant de manière significative de façon similaire*[12]*;*
- *b) le 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*[13]*; ou*
- *c) la surveillance systématique à grande échelle d'une zone accessible au public»*.

Comme le laissent entendre les mots *«en particulier»* dans la phrase introductive de l'article 35, paragraphe 3, du RGPD, il s'agit là d'une liste non exhaustive. Même si elles ne figurent pas dans cette liste, d'autres opérations de traitement peuvent néanmoins présenter un risque aussi élevé. Ces opérations de traitement doivent également faire l'objet d'une AIPD. C'est la raison pour laquelle les critères exposés ci-dessous vont parfois au-delà d'une simple explication de ce que les trois exemples de l'article 35, paragraphe 3, du RGPD donnent à comprendre.

Pour donner une vision plus concrète des opérations de traitement qui nécessitent une AIPD du fait d'un risque inhérent élevé, compte tenu des éléments particuliers de l'article 35, paragraphes 1 et 3, points a) à c), de la liste à adopter au niveau national en vertu de l'article 35, paragraphe 4, et des considérants 71, 75 et 91, ainsi que des autres références du RGPD aux opérations de traitement «*susceptibles d'engendrer un risque élevé»*[14], il convient de prendre en compte les neuf critères ci-après.

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*» (considérants 71 et 91). 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.

---

[12] Voir le considérant 75: «*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*».

[13] Voir le considérant 75: «*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*».

[14] Voir par exemple les considérants 75, 76, 92 et 116.

2. Prise de décisions automatisée avec effet juridique ou effet similaire significatif: traitement ayant pour finalité la prise de décisions à l'égard des personnes concernées produisant «*des effets juridiques à l'égard d'une personne physique ou l'affectant de manière significative de façon similaire*» [article 35, paragraphe 3, point a)]. Le traitement pourrait, par exemple, entraîner l'exclusion ou une discrimination. Les traitements n'ayant que peu ou pas d'effet sur les personnes ne répondent pas à ce critère particulier. Des explications complémentaires concernant ces notions seront fournies dans les prochaines lignes directrices du GT29 relatives au profilage.
3. Surveillance systématique: traitement utilisé pour observer, surveiller ou contrôler les personnes concernées, y compris la collecte de données via des réseaux ou par «*la surveillance systématique […] d'une zone accessible au public*» [article 35, paragraphe 3, point c)][15]. Ce type de surveillance est 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 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.
4. Données sensibles ou données à caractère hautement personnel: il s'agit de 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. 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. Au-delà des dispositions du RGPD, certaines catégories de données peuvent être considérées comme augmentant le risque possible pour les droits et libertés des personnes. Ces données à caractère personnel sont considérées comme sensibles (au sens commun du terme) 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 met en cause la liberté de circulation, par exemple) ou dans la mesure où leur violation 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). À cet égard, il peut être pertinent de déterminer si les données ont déjà été rendues publiques par la personne concernée ou par des tiers. Le fait que les données à caractère personnel soient publiquement disponibles peut être pris en compte en tant que facteur dans l'analyse lorsqu'il est prévu une utilisation ultérieure des données pour certaines finalités. Ce critère peut également inclure les données telles que les documents personnels, les courriers électroniques, les agendas, les notes des liseuses équipées

[15] Pour le GT29, s'entend comme «*systématique*» toute surveillance qui remplit un ou plusieurs des critères suivants (voir les lignes directrices 16/EN WP 243 du GT29 relatives aux délégués à la protection des données):

- se déroule selon un système;
- préparée, organisée ou méthodique;
- se déroule dans le cadre d'un plan général de collecte de données;
- réalisée dans le cadre d'une stratégie.

Pour le GT29, s'entend comme une «*zone accessible au public*» tout 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.

de fonctions de prise de notes ainsi que les informations à caractère très personnel contenues dans les applications de «life-logging».

5. Données traitées à grande échelle: le RGPD ne précise pas ce qu'il faut entendre par «grande échelle», même si le considérant 91 fournit quelques indications à ce sujet. Quoi qu'il en soit, pour déterminer si le traitement est effectué à grande échelle, le GT29 recommande de prendre en compte, en particulier, les facteurs suivants:[16]
    a. le nombre de personnes concernées, soit en valeur absolue, soit en proportion de la population considérée;
    b. le volume de données et/ou l'éventail des différents éléments de données traitées;
    c. la durée ou la permanence de l'activité de traitement de données;
    d. l'étendue géographique de l'activité de traitement.
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[17].
7. Données concernant des personnes vulnérables (considérant 75): 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. Peuvent être considérés comme des personnes concernées vulnérables, les enfants (qui peuvent être vus comme incapables de s'opposer ou de consentir sciemment et de manière réfléchie au traitement de leurs données), les employés, les segments les plus vulnérables de la population nécessitant une protection particulière (personnes souffrant de maladie mentale, demandeurs d'asile et personnes âgées, patients, etc.) et, en tout état de cause, toutes autres personnes pour lesquelles un déséquilibre dans la relation avec le responsable du traitement peut être identifié.
8. Utilisation innovante ou application de nouvelles solutions technologiques ou organisationnelles: utilisation combinée, par exemple, de systèmes de reconnaissance des empreintes digitales et de reconnaissance faciale pour améliorer le contrôle des accès physiques, etc. Le RGPD indique clairement (article 35, paragraphe 1, et considérants 89 et 91) que l'utilisation d'une nouvelle technologie, définie en «*conformité avec l'état des connaissances technologiques*» (considérant 91), peut déclencher la nécessité d'une AIPD, et ce en raison du fait 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. En effet, les conséquences personnelles et sociales du déploiement d'une nouvelle technologie peuvent être inconnues, et une AIPD aidera le responsable du traitement à comprendre et à traiter de tels risques. Par exemple, certaines applications de «l'internet des objets» sont susceptibles d'avoir un impact important sur la vie quotidienne et la vie privée des personnes, et nécessitent par conséquent une AIPD.
9. Traitements en eux-mêmes qui «*empêchent [les personnes concernées] d'exercer un droit ou de bénéficier d'un service ou d'un contrat*» (article 22 et considérant 91). Ces traitements incluent notamment les opérations visant à autoriser, modifier ou refuser l'accès à un service ou la conclusion d'un contrat. À titre d'exemple, prenons le cas d'une banque passant ses

[16] Voir les lignes directrices 16/EN WP 243 du GT29 relatives aux délégués à la protection des données.

[17] Voir l'explication fournie dans l'avis 13/EN WP 203 du GT29 relatif à la limitation des finalités, p. 24.

clients au crible d'une base de données de cote de crédit avant d'arrêter ses décisions d'octroi de prêt.

Dans la plupart des cas, le responsable du traitement peut considérer qu'un traitement satisfaisant à deux critères nécessite une AIPD. D'une manière générale, le GT29 estime que plus le traitement remplit de critères, plus il est susceptible de présenter un risque élevé pour les droits et libertés des personnes concernées et par conséquent de nécessiter une AIPD, quelles que soient les mesures que le responsable du traitement envisage d'adopter.

Néanmoins, dans certains cas, **le responsable du traitement peut considérer que même si son traitement ne satisfait qu'à un seul de ces critères, il requiert malgré tout une AIPD.**

Les exemples qui suivent illustrent la façon dont il convient d'utiliser les critères pour déterminer si une opération de traitement considérée nécessite une AIPD.

Exemples d'opérations de traitement	**Critères potentiellement pertinents**	**AIPD potentiellement requise?**
Traitement par un hôpital des données génétiques et des données de santé de ses patients (système d'information hospitalier).	- Données sensibles ou données à caractère hautement personnel. - Données concernant des personnes vulnérables. - Données traitées à grande échelle.	Oui
Utilisation d'un système de caméras pour surveiller les comportements routiers. Le responsable du traitement envisage d'utiliser un système d'analyse vidéo intelligente pour isoler les véhicules et reconnaître automatiquement les plaques d'immatriculation.	- Surveillance systématique. - Utilisation innovante ou application de solutions technologiques ou organisationnelles.	
Surveillance systématique par une entreprise des activités de ses employés, y compris leur poste de travail, leur activité sur internet, etc.	- Surveillance systématique. - Données concernant des personnes vulnérables.	
Collecte de données sur les réseaux sociaux publics dans le but de générer des profils.	- Évaluation ou notation. - Données traitées à grande échelle. - Croisement ou combinaison d'ensembles de données. - Données sensibles ou données à caractère hautement personnel.	
Création par une institution d'une base de données spécialisée dans la notation de crédit ou «antifraude» au niveau national.	- Évaluation ou notation. - Prise de décisions automatisée avec effet juridique ou effet similaire significatif. - Empêche les personnes concernées d'exercer un droit ou de bénéficier d'un service ou d'un contrat. - Données sensibles ou données à caractère hautement personnel.	
Stockage à des fins d'archivage de données à	- Données sensibles.	

Exemples d'opérations de traitement	Critères potentiellement pertinents	AIPD potentiellement requise?
caractère personnel sensibles, pseudonymisées, concernant des personnes vulnérables participant à des projets de recherche ou à des essais cliniques.	- Données concernant des personnes vulnérables. - Empêche les personnes concernées d'exercer un droit ou de bénéficier d'un service ou d'un contrat.	
Traitement de «données à caractère personnel de patients ou de clients par un médecin, un autre professionnel de la santé ou un avocat exerçant à titre individuel» (considérant 91).	- Données sensibles ou données à caractère hautement personnel. - Données concernant des personnes vulnérables.	Non
Utilisation par un magazine en ligne d'une liste de diffusion pour communiquer à ses abonnés son digest générique quotidien.	- Données traitées à grande échelle.	
Diffusion par un site de commerce électronique de publicités pour des pièces automobiles anciennes impliquant un profilage limité, basé sur les articles visualisés ou achetés sur le site internet.	- Évaluation ou notation.	

À l'inverse, une opération de traitement peut correspondre à l'un des cas susmentionnés et être néanmoins considérée par le responsable du traitement comme non «susceptible d'engendrer un risque élevé». Dans pareil cas, il convient que le responsable du traitement explique et documente les motifs de sa décision de ne pas procéder à une AIPD en incluant/rapportant par ailleurs l'opinion à cet égard du délégué à la protection des données.

De plus, dans le cadre du principe de responsabilité, il est prévu que les responsables du traitement «*tiennent un registre des activités de traitement effectuées sous leur responsabilité*», lequel doit consigner un certain nombre d'informations, dont les finalités du traitement, une description des catégories de données concernées et des destinataires des données et «*dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles visées à l'article 32, paragraphe 1*» (article 30, paragraphe 1), et chacun d'eux a l'obligation d'évaluer la probabilité d'un risque élevé, y compris s'il décide finalement de ne pas effectuer d'AIPD.

Remarque: les autorités de contrôle sont tenues d'établir, de publier et de communiquer au Comité européen de la protection des données (CEPD) une liste des opérations de traitement nécessitant une AIPD (article 35, paragraphe 4)[18]. Les critères susmentionnés peuvent aider les autorités de contrôle à constituer une telle liste, à laquelle d'autres éléments spécifiques pourront être intégrés en temps voulu, le cas échéant. Par exemple, le traitement de tout type de données biométriques ainsi que celui

[18] Dans ce contexte, «*l'autorité de contrôle compétente applique le mécanisme de contrôle de la cohérence visé à l'article 63, lorsque ces listes comprennent 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*» (article 35, paragraphe 6).

des données des enfants pourraient également être considérés comme pertinents aux fins de l'établissement de la liste visée à l'article 35, paragraphe 4.

b) Quand une AIPD n'est-elle pas nécessaire? Lorsque le traitement n'est pas *«susceptible d'engendrer un risque élevé»* ou qu'une AIPD similaire existe déjà ou que le traitement a été autorisé avant mai 2018 ou qu'il a une base juridique ou encore qu'il figure dans la liste des opérations de traitement qui ne requièrent pas d'AIPD.

Le GT29 considère qu'une AIPD n'est pas nécessaire dans les cas suivants:

- **lorsque le traitement n'est pas «*susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques*»** (article 35, paragraphe 1);
- **lorsque le traitement est très similaire en termes de nature, de portée, de contexte et de finalités à un autre traitement qui a fait l'objet d'une AIPD.** Dans un tel cas, les résultats de l'AIPD réalisée pour le traitement similaire peuvent être utilisés (article 35, paragraphe 1[19]);
- lorsque le traitement a fait l'objet d'un examen mené par une autorité de contrôle avant mai 2018 dans des conditions spécifiques qui n'ont pas changé[20] (voir III, C);
- **lorsque le traitement,** effectué en application de l'article 6, paragraphe 1, point c) ou e), **a une base juridique** dans le droit de l'Union ou dans le droit de l'État membre, que ce droit règlemente l'opération de traitement spécifique **et qu'une AIPD a déjà été réalisée** dans le cadre de l'établissement de la base juridique en question (article 35, paragraphe 10)[21], à moins qu'un État membre n'estime qu'il est nécessaire de procéder à une telle analyse avant les activités de traitement;
- **lorsque le traitement figure dans la liste facultative (établie par l'autorité de contrôle) des opérations de traitement** qui ne requièrent pas d'AIPD (article 35, paragraphe 5). Cette liste peut recenser les activités de traitement conformes aux conditions fixées par l'autorité en question, en particulier par l'intermédiaire de lignes directrices, de décisions ou autorisations spécifiques, de règles de conformité, etc. (par ex. en France, autorisations, dispenses, règles simplifiées, packs de conformité...). Dans pareil cas et sous réserve d'une réévaluation par l'autorité de contrôle compétente, il n'est pas nécessaire d'effectuer une AIPD, à la condition exclusive, toutefois, que le traitement relève strictement du champ d'application de la procédure pertinente indiquée dans la liste et continue de satisfaire pleinement à toutes les exigences applicables du RGPD.

C. <u>Et qu'en est-il des opérations de traitement déjà existantes? Une AIPD est nécessaire dans certains cas.</u>

[19] «*Une seule et même analyse peut porter sur un ensemble d'opérations de traitement similaires qui présentent des risques élevés similaires*».

[20] «*Les décisions de la Commission qui ont été adoptées et 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*» (considérant 171).

[21] 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.

L'obligation d'effectuer une AIPD s'applique aux opérations de traitement existantes susceptibles d'engendrer un risque élevé pour les droits et libertés des personnes physiques et pour lesquelles les risques associés ont évolué, compte tenu de la nature, de la portée, du contexte et des finalités du traitement.

Aucune AIPD n'est nécessaire pour les opérations de traitement qui ont fait l'objet d'un examen par une autorité de contrôle ou par le détaché à la protection des données, conformément à l'article 20 de la directive 95/46/CE, et dont la mise en œuvre n'a pas changé depuis le contrôle préalable. En effet, «*Les décisions de la Commission qui ont été adoptées et 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*» (considérant 171).

À l'inverse, ceci signifie que tout traitement de données dont les conditions de mise en œuvre (portée, finalités, données à caractère personnel collectées, identité des responsables du traitement ou des destinataires des données, durée de conservation des données, mesures techniques et organisationnelles, etc.) ont changé depuis l'examen préalable effectué par l'autorité de contrôle ou le détaché à la protection des données et sont susceptibles d'engendrer un risque élevé doit faire l'objet d'une AIPD.

De plus, une AIPD peut être nécessaire à la suite d'une évolution des risques découlant des opérations de traitement[22], par exemple en raison du recours à une nouvelle technologie ou de l'utilisation des données à caractère personnel à des fins différentes. Les opérations de traitement peuvent évoluer rapidement et de nouvelles vulnérabilités peuvent apparaître. Par conséquent, il convient de noter que la révision d'une AIPD est non seulement utile dans un souci d'amélioration continue, mais également essentielle pour maintenir le niveau de protection des données dans un environnement qui change au fil du temps. Une AIPD peut également devenir nécessaire du fait d'une évolution du contexte organisationnel ou sociétal de l'activité 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.

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.

À titre de bonne pratique, **une AIPD devrait faire l'objet d'un examen continu et être régulièrement réévaluée.** Par conséquent, même si une AIPD ne s'avère pas nécessaire le 25 mai 2018, il conviendra, le moment venu, que le responsable du traitement procède à une telle AIPD dans le cadre de ses obligations générales de responsabilité.

D. Comment effectuer une AIPD?

a) Quand convient-il d'effectuer une AIPD? Préalablement au lancement du traitement.

[22] Eu égard aux différents aspects suivants: contexte, données collectées, finalités, fonctionnalités, données à caractère personnel traitées, destinataires, combinaisons de données, risques (actifs de soutien, sources de risques, impacts potentiels, menaces, etc.), mesures de sécurité et transferts internationaux.

L'AIPD doit être effectuée «*avant le traitement*» (article 35, paragraphes 1 et 10, considérants 90 et 93)[23]. Cette exigence est cohérente avec les principes de protection des données dès la conception et de protection des données par défaut (article 25 et considérant 78). L'AIPD doit être considérée comme un outil d'aide à la prise de décisions en ce qui concerne le traitement.

L'AIPD doit être lancée le plus tôt possible dans le cycle de conception du traitement, même si certaines opérations de traitement sont encore inconnues. La mise à jour de l'AIPD tout au long du projet assurera la prise en compte des questions liées à la protection des données et de la vie privée et encouragera la création de solutions favorisant la conformité. Il peut également être nécessaire de répéter les différentes étapes de l'évaluation au fur et à mesure de l'avancée du processus de développement étant donné que le choix de certaines mesures techniques ou organisationnelles peut modifier la gravité ou la probabilité des risques associés au traitement.

Le fait que l'AIPD puisse devoir être actualisée après le lancement effectif du traitement n'est pas une raison valable pour la différer ou pour ne pas l'effectuer. Une telle analyse est un processus continu, en particulier lorsque l'opération de traitement est dynamique et soumise à de constants changements. **La réalisation d'une AIPD relève d'un processus continu et n'est pas un exercice ponctuel**.

b) Qui est tenu d'effectuer l'AIPD? Le responsable du traitement, avec le DPD et les sous-traitants.

La responsabilité de veiller à ce qu'une AIPD soit effectuée incombe au responsable du traitement (article 35, paragraphe 2). 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.

Le responsable du traitement est également tenu de prendre conseil auprès du délégué à la protection des données (DPD), si un tel délégué a été désigné (article 35, paragraphe 2), et il convient que l'AIPD documente les conseils ainsi recueillis ainsi que les décisions prises par le responsable du traitement. Le DPD a également pour mission de vérifier l'exécution de l'AIPD [article 39, paragraphe 1, point c)]. Des précisions complémentaires sont fournies dans les lignes directrices 16/EN WP 243 du GT29 relatives aux délégués à la protection des données.

Si le traitement est entièrement ou partiellement effectué par un sous-traitant, **ce dernier doit aider le responsable du traitement à effectuer l'AIPD** et fournir toutes les informations nécessaires [en application de l'article 28, paragraphe 3, point f)].

Le responsable du traitement «*demande l'avis des personnes concernées ou de leurs représentants*» (article 35, paragraphe 9), «*le cas échéant*». Le GT29 considère que:

- ces avis peuvent être recueillis par divers moyens, selon le contexte (par ex. une étude générique en lien avec les finalités et les moyens de l'opération de traitement, un questionnaire soumis aux représentants du personnel, ou des enquêtes de type habituel envoyées aux futurs clients du responsable du traitement), le responsable du traitement devant s'assurer de s'appuyer sur une base juridique pour le traitement de toutes données à caractère personnel

[23] À moins qu'il s'agisse d'un traitement déjà existant ayant préalablement fait l'objet d'un examen par l'autorité de contrôle, auquel cas l'AIPD sera effectuée avant toute mise en œuvre de modifications significatives.

impliquées dans cette collecte d'avis. Il convient toutefois de noter que demander le consentement au traitement n'est évidemment pas un moyen de recueillir l'avis des personnes concernées;

- 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;
- le responsable du traitement doit également justifier toute décision de ne pas recueillir l'avis des personnes concernées s'il juge la démarche inappropriée, en estimant par exemple que cela compromettrait la confidentialité de plans d'affaires ou serait disproportionné ou irréalisable.

Enfin, il est de bonne pratique de définir et de documenter les autres rôles et responsabilités spécifiques, en fonction de la politique interne et des processus et règles en jeu; 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[24] (avocats, experts en informatique, experts en sécurité, sociologues, experts en déontologie, etc.);
- les rôles et responsabilités de tout sous-traitant doivent être définis contractuellement, et l'AIPD doit être effectuée avec son aide, compte tenu de la nature du traitement et des informations à la disposition du sous-traitant (article 28, paragraphe 3, point f)];
- 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.

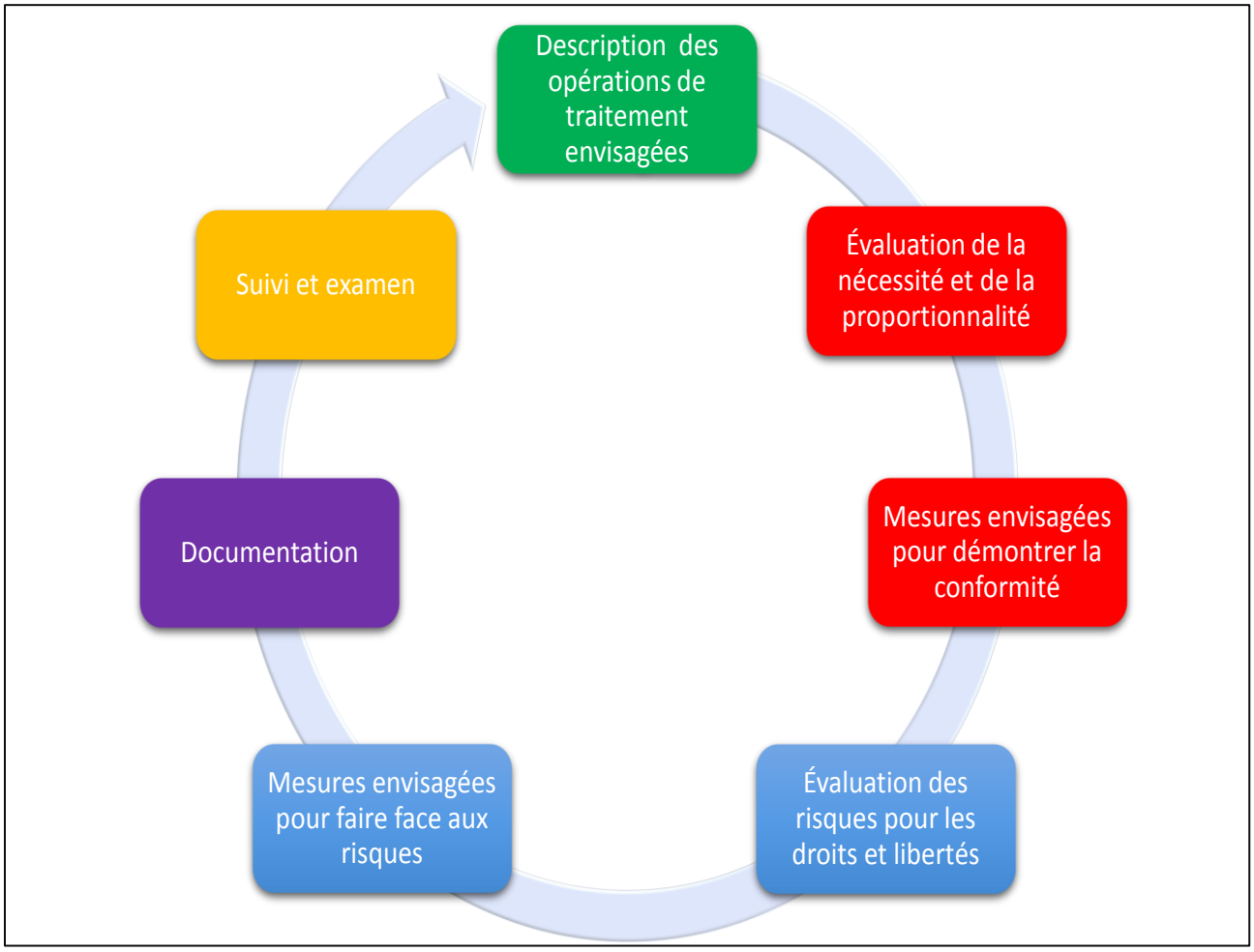
c) Quelle est la méthodologie à suivre pour effectuer une AIPD? Différentes méthodologies mais des critères communs.

[24] *Recommendations for a privacy impact assessment framework for the European Union, Deliverable D3:* http://www.piafproject.eu/ref/PIAF_D3_final.pdf.

Le RGPD dispose qu'une AIPD (article 35, paragraphe 7, et considérants 84 et 90) doit au moins contenir:

- «*une description systématique des opérations de traitement envisagées et des finalités du traitement*»;
- «*une évaluation de la nécessité et de la proportionnalité des opérations de traitement*»;
- «*une évaluation des risques pour les droits et libertés des personnes concernées*»;
- «*les mesures envisagées pour:*
  - «*faire face aux risques*»;
  - «*apporter la preuve du respect [du] règlement*».

Le schéma suivant illustre le processus itératif générique suggéré pour la réalisation d'une AIPD[25]:



Le respect d'un code de conduite (article 40) doit être pris en compte (article 35, paragraphe 8) lors de l'évaluation de l'impact d'une opération de traitement de données. Ceci peut être utile pour démontrer que des mesures adéquates ont été choisies ou mises en place, à condition toutefois que le code de conduite soit approprié pour l'opération de traitement considérée. Il convient également de prendre en

[25] Il convient de souligner que le processus décrit ici est itératif: dans la pratique, chacune des étapes devra probablement être réexaminée plusieurs fois avant que l'AIPD ne puisse être finalisée.

compte les garanties que représentent les certifications, labels et marques destinés à démontrer la conformité au RGPD des opérations de traitement effectuées par les responsables du traitement et les sous-traitants (article 42) ainsi que l'application de règles d'entreprise contraignantes (REC).

Toutes les exigences pertinentes établies dans le RGPD fournissent un cadre général et générique pour la conception et la réalisation d'une AIPD. La mise en œuvre pratique de l'AIPD sera dès lors fonction des exigences du RGPD pouvant être complétées par des indications pratiques plus détaillées. La mise en œuvre d'une AIPD est donc en ce sens adaptable. Cela signifie que même un responsable du traitement opérant sur de petites quantités de données peut concevoir et mettre en œuvre une AIPD adaptée à ses opérations de traitement.

Le considérant 90 du RGPD mentionne un certain nombre d'éléments d'une AIPD qui recouvrent des composantes bien définies de la gestion des risques (par ex. dans la norme ISO 31000[26]). En termes de gestion des risques, une AIPD a pour objectif d'aider à «gérer les risques» pour les droits et libertés des personnes physiques en:

- établissant le contexte: «*compte tenu de la nature, de la portée, du contexte et des finalités du traitement et des sources du risque*»;
- appréciant le risque: «*évaluer la probabilité et la gravité particulières du risque élevé*»;
- traitant le risque: «*atténuer ce risque*» et «*assurer la protection des données à caractère personnel*», et «*démontrer le respect du présent règlement*».

Remarque: l'AIPD au sens du RGPD est un outil de gestion des risques pour les droits des personnes concernées et se place ainsi sous l'angle de leurs droits, comme c'est également le cas dans certains autres domaines tels que la sécurité sociétale, par exemple. À l'inverse, dans d'autres domaines encore (par ex. la sécurité de l'information), la gestion des risques est axée sur l'organisation.

La souplesse offerte par le RGPD permet au responsable du traitement de déterminer la structure et la forme précises de l'AIPD afin qu'elles soient adaptées aux pratiques de travail existantes. Il existe un certain nombre de processus établis au sein de l'UE et dans le monde qui tiennent compte des éléments décrits au considérant 90. Cependant, quelle que soit sa forme, une AIPD se doit d'être une véritable évaluation des risques, permettant au responsable du traitement de prendre des mesures pour y faire face.

Différentes méthodologies (voir l'annexe 1 pour des exemples de méthodologies d'analyse d'impact sur la protection des données et la vie privée) peuvent être utilisées pour faciliter la mise en œuvre des exigences de base énoncées dans le RGPD. Afin de permettre le développement de ces différentes approches, tout en aidant les responsables du traitement à respecter les dispositions du RGPD, des critères communs ont été identifiés (voir l'annexe 2). Ces derniers clarifient les exigences de base du règlement, mais offrent suffisamment de marge de manœuvre pour autoriser différentes formes de mise en œuvre. Ces critères peuvent être utilisés pour démontrer qu'une méthodologie d'AIPD considérée satisfait aux normes établies par le RGPD. **Il appartient au responsable du traitement de choisir une méthodologie, mais cette méthodologie doit satisfaire aux critères visés à l'annexe 2.**

[26] Processus de gestion des risques: communication et consultation, établissement du contexte, appréciation du risque, traitement du risque, suivi et évaluation (voir la section Termes et définitions et la table des matières dans l'aperçu de la norme ISO 31000: https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-1:v1:en).

Le GT29 encourage le développement de cadres sectoriels pour les AIPD qui, dans la mesure où ils se fondent sur des connaissances sectorielles spécifiques, permettent dès lors à l'AIPD de prendre en compte les spécificités d'un type particulier d'opération de traitement (par ex.: types particuliers de données, d'actifs d'entreprise, d'impacts potentiels, de menaces, de mesures). L'AIPD est ainsi en mesure de traiter les problèmes qui se posent dans un secteur économique donné, ou lors de l'utilisation de technologies particulières ou encore de l'exécution de types particuliers d'opérations de traitement.

Enfin, si nécessaire, «*le responsable du traitement procède à un examen afin d'évaluer si le traitement est effectué conformément à l'analyse d'impact relative à la protection des données, au moins quand il se produit une modification du risque présenté par les opérations de traitement*» (article 35, paragraphe 11[27]).

d) Est-il obligatoire de publier l'AIPD? Non, mais la publication d'un résumé peut être de nature à susciter la confiance, et l'AIPD complète doit être communiquée à l'autorité de contrôle en cas de consultation préalable ou sur demande de l'APD.

Le RGPD ne fait pas obligation de publier l'AIPD, et il relève de la discrétion du responsable du traitement de la publier ou non. Cependant, une publication au moins partielle, sous la forme d'un résumé ou d'une conclusion de son AIPD, devrait être envisagée par le responsable du traitement.

Une telle pratique serait utile pour susciter la confiance dans les opérations de traitement du responsable du traitement et pour donner des gages de responsabilité et 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.

L'AIPD publiée n'a pas besoin d'inclure l'intégralité de l'analyse, notamment lorsque celle-ci pourrait donner 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 pareille situation, 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.

De plus, lorsqu'une AIPD révèle des risques résiduels élevés, le responsable du traitement est tenu de se tourner vers l'autorité de contrôle pour une consultation préalable concernant le traitement (article 36, paragraphe 1). Dans le cadre cette dernière, l'AIPD doit être communiquée dans son intégralité [article 36, paragraphe 3, point e)]. L'autorité de contrôle peut fournir un avis[28], et veillera à protéger le secret des affaires et à ne pas divulguer de vulnérabilités dans la sécurité, sous réserve des principes applicables dans chaque État membre en matière d'accès du public aux documents officiels.

E. <u>Quand convient-il de consulter l'autorité de contrôle? En présence de risques résiduels élevés.</u>

[27] Seule l'application des paragraphes 1 à 7 de l'article 35 est explicitement exclue par l'article 35, paragraphe 10.

[28] La communication d'un avis écrit au responsable du traitement n'est nécessaire que si l'autorité de contrôle juge que le traitement envisagé ne respecte pas les dispositions du règlement, conformément à l'article 36, paragraphe 2.

Comme expliqué précédemment:

- une AIPD est requise lorsque le traitement «*est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques*» [article 35, paragraphe 1; voir III, B, a)]. À titre d'exemple, le traitement de données de santé à grande échelle est considéré comme susceptible d'engendrer un risque élevé et nécessite une AIPD;
- dès lors, il appartient au responsable du traitement d'évaluer les risques pour les droits et libertés des personnes concernées et d'identifier les mesures[29] envisagées pour réduire ces risques à un niveau acceptable et apporter la preuve du respect du RGPD [article 35, paragraphe 7; voir III, C, c)]. Par exemple, dans un cas de stockage de données à caractère personnel sur ordinateurs portables, l'application de mesures de sécurité techniques et organisationnelles appropriées (chiffrement efficace et complet des disques, gestion des clés rigoureuse, contrôle approprié des accès, sauvegardes sécurisées, etc.) en plus des règles existantes (avis, consentement, droit d'accès, droit d'opposition, etc.).

Dans l'exemple des ordinateurs portables ci-dessus, à condition que les risques aient été jugés suffisamment réduits par le responsable du traitement et après prise en compte de l'article 36, paragraphe 1, et des considérants 84 et 94, le traitement pourrait être mis en œuvre sans consultation de l'autorité de contrôle. Ce n'est que lorsque les risques identifiés ne peuvent pas être suffisamment réduits par le responsable du traitement (à savoir en présence de risques résiduels élevés) que ce dernier est tenu de consulter l'autorité de contrôle.

Un risque résiduel peut notamment être considéré comme élevé et inacceptable dès lors qu'il exposerait les personnes à des conséquences importantes, voire irréversibles, qu'elles seraient susceptibles de ne pas pouvoir surmonter (par ex:. un accès illégitime à leurs données qui pourrait menacer leur vie, entraîner une mise à pied, mettre en péril leur situation financière) et/ou lorsqu'il semble évident que le risque se concrétisera (par ex.: 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).

Lorsque le responsable du traitement ne parvient pas à identifier des mesures suffisantes pour réduire les risques à un niveau acceptable (à savoir que les risques résiduels demeurent élevés), une consultation de l'autorité de contrôle est obligatoire[30].

En outre, l'autorité de contrôle devra être consultée dans tous les cas où le droit de l'État membre exige que les responsables du traitement consultent l'autorité de contrôle et/ou obtiennent son autorisation préalable en ce qui concerne un traitement que le responsable du traitement envisage dans le cadre d'une mission d'intérêt public dont il est investi, notamment pour les traitements en rapport avec la protection sociale et la santé publique (article 36, paragraphe 5).

[29] En tenant également compte des orientations existantes du CEPD et des autorités de contrôle, ainsi que des possibilités techniques les plus récentes et des coûts de mise en œuvre, comme prévu à l'article 35, paragraphe 1.

[30] Remarque: «*la pseudonymisation et le chiffrement des données à caractère personnel*» (tout comme la minimisation des données, les mécanismes de contrôle, etc.) ne sont pas nécessairement des mesures appropriées. Il ne s'agit là que d'exemples. Les mesures appropriées dépendent du contexte et des risques spécifiques aux opérations de traitement.

Il convient toutefois de noter que, indépendamment de la nécessité ou non de consulter l'autorité de contrôle en fonction du niveau du risque résiduel, les obligations de conserver un rapport de l'AIPD et de mettre celle-ci à jour en temps utile demeurent.

IV. Conclusions et recommandations

Les AIPD sont un outil utile pour les responsables du traitement aux fins de l'établissement de systèmes de traitement de données répondant aux exigences du RGPD et peuvent être obligatoires pour certains types d'opérations de traitement. Leur mise en œuvre est adaptable et elles peuvent prendre différentes formes, même si le RGPD fixe les conditions de base à remplir pour une AIPD effective. La réalisation d'une AIPD devrait être considérée par les responsables du traitement comme une activité utile et positive aidant à se conformer à la législation.

L'article 24, paragraphe 1, définit comme suit la responsabilité fondamentale du responsable du traitement aux fins du respect du RGPD: «*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 met en œuvre des mesures techniques et organisationnelles appropriées pour s'assurer et être en mesure de démontrer que le traitement est effectué conformément au présent règlement. Ces mesures sont réexaminées et actualisées si nécessaire*».

L'AIPD est un élément essentiel de la mise en conformité avec le règlement lorsqu'un traitement de données à risque élevé est prévu ou déjà effectué. Il convient par conséquent que les responsables du traitement utilisent les critères définis dans le présent document pour déterminer si une AIPD est ou non nécessaire. Dans sa politique interne, le responsable du traitement peut étendre cette liste au-delà des obligations légales fixées par le RGPD, ce qui pourra lui attirer une confiance accrue de la part des personnes concernées et des autres responsables du traitement.

Lorsqu'un traitement à risque potentiellement élevé est prévu, le responsable du traitement doit:

- choisir une méthodologie d'AIPD (voir les exemples donnés à l'annexe 1) qui satisfait aux critères de l'annexe 2, ou spécifier et mettre en œuvre un processus d'AIPD systématique:
  - conforme aux critères de l'annexe 2;
  - intégré aux processus existants de conception, de développement, de modification, de gestion des risques et d'examen opérationnel, selon les processus, le contexte et la culture internes;
  - impliquant les parties intéressées et définissant clairement leurs responsabilités (responsable du traitement, DPD, personnes concernées ou leurs représentants, unités opérationnelles, services techniques, sous-traitants, responsable de la sécurité des systèmes d'information, etc.);
- communiquer son rapport d'AIPD à l'autorité de contrôle compétente si la demande lui en est faite;
- consulter l'autorité de contrôle s'il n'a pas réussi à identifier des mesures suffisantes pour atténuer les risques élevés;
- procéder à un réexamen périodique de l'AIPD et du traitement qu'elle évalue, au moins lorsqu'un changement intervient dans les risques présentés par le traitement;
- documenter les décisions prises.

Annexe 1 — Exemples de cadres européens existants pour la réalisation d'une AIPD

Le RGPD ne précise pas la procédure à suivre pour effectuer une AIPD et laisse le loisir aux responsables du traitement de recourir à un cadre qui complète leurs pratiques de travail existantes, sous réserve néanmoins que celui-ci prenne en compte les éléments décrits à l'article 35, paragraphe 7. Il peut s'agir d'un cadre sur mesure pour le responsable du traitement ou commun à un secteur particulier. Un certain nombre de cadres développés par les APD de l'UE ainsi que de cadres sectoriels européens ont été publiés, dont en particulier les suivants:

Exemples de cadres européens génériques:

- DE: Standard Data Protection Model, V.1.0 – Trial version, 2016[31].
  https://www.datenschutzzentrum.de/uploads/SDM-Methodology_V1_EN1.pdf
- ES: *Guía para una Evaluación de Impacto en la Protección de Datos Personales (EIPD)*, Agencia española de protección de datos (AGPD), 2014.
  https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/Guia_EIPD.pdf
- FR: *Étude d'impacts sur la vie privée (PIA)*, Commission nationale de l'informatique et des libertés (CNIL), 2015.
  https://www.cnil.fr/fr/etude-dimpacts-sur-la-vie-privee-suivez-la-methode-de-la-cnil
- UK: *Conducting privacy impact assessments code of practice*, Information Commissioner's Office (ICO), 2014.
  https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf

Exemples de cadres européens sectoriels:

- Cadre relatif à l'analyse de l'impact sur la vie privée et la protection des données pour les applications RFID [32].
  http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp180_annex_en.pdf
- Modèle d'analyse d'impact sur la protection des données des réseaux intelligents et des systèmes intelligents de mesure [33]
  http://ec.europa.eu/energy/sites/ener/files/documents/2014_dpia_smart_grids_forces.pdf

---

[31] Unanimement et positivement adopté (avec l'abstention de la Bavière) par la 92e conférence des autorités indépendantes pour la protection des données du Bund et des Länder qui s'est tenue à Kühlungsborn les 9 et 10 novembre 2016.

[32] Voir aussi:

- la recommandation de la Commission du 12 mai 2009 sur la mise en œuvre des principes de respect de la vie privée et de protection des données dans les applications reposant sur l'identification par radiofréquence;
  http://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:32009H0387&from=FR
- l'avis 9/2011 sur la proposition révisée des entreprises relative au cadre d'évaluation de l'impact sur la protection des données et de la vie privée des applications reposant sur l'identification par radiofréquence (RFID).
  http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp180_fr.pdf

[33] Voir aussi l'avis 07/2013 sur le modèle d'analyse d'impact relative à la protection des données pour les réseaux intelligents et les systèmes de relevés intelligents (modèle d'AIPD) élaboré par le groupe d'experts 2 de la task-force sur les réseaux intelligents de la Commission. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp209_fr.pdf

Une norme internationale fournit également des lignes directrices concernant les méthodologies applicables pour la réalisation d'une AIPD (ISO/IEC 29134[34]).

[34] ISO/IEC 29134 (projet, indisponible en français), *Technologies de l'information – Techniques de sécurité – Lignes directrices pour l'évaluation d'impacts sur la vie privée*, Organisation internationale de normalisation (ISO).

Annexe 2 — Critères d'acceptabilité d'une AIPD

Les critères suivants proposés par le GT29 peuvent être utilisés par les responsables du traitement pour déterminer si une AIPD ou une méthodologie d'AIPD considérée est suffisamment complète aux fins du respect des exigences du RGPD:

- ☐ une description systématique du traitement est fournie [article 35, paragraphe 7, point a)]:
  - ☐ la nature, la portée, le contexte et les finalités du traitement sont pris en compte (considérant 90);
  - ☐ les données à caractère personnel concernées, les destinataires et la durée pendant laquelle les données à caractère personnel seront conservées sont précisés;
  - ☐ une description fonctionnelle de l'opération de traitement est fournie;
  - ☐ les actifs sur lesquels reposent les données à caractère personnel (matériels, logiciels, réseaux, personnes, documents papier ou canaux de transmission papier) sont identifiés;
  - ☐ le respect de codes de conduite approuvés est pris en compte (article 35, paragraphe 8);
- ☐ la nécessité et la proportionnalité sont évaluées [article 35, paragraphe 7, point b)]:
  - ☐ les mesures envisagées pour assurer la conformité au règlement sont déterminées [article 35, paragraphe 7, point d), et considérant 90], avec prise en compte:
    - ☐ de mesures contribuant au respect des principes de proportionnalité et de nécessité du traitement, fondées sur les exigences suivantes:
      - ☐ finalités déterminées, explicites et légitimes (article 5, paragraphe 1, point b)];
      - ☐ licéité du traitement (article 6);
      - ☐ données adéquates, pertinentes et limitées à ce qui est nécessaire [article 5, paragraphe 1, point c)];
      - ☐ durée de conservation limitée [article 5, paragraphe 1, point e)];
    - ☐ de mesures contribuant aux droits des personnes concernées:
      - ☐ informations fournies à la personne concernée (articles 12, 13 et 14);
      - ☐ droit d'accès et droit à la portabilité des données (articles 15 et 20);
      - ☐ droit de rectification et droit à l'effacement (articles 16, 17 et 19);
      - ☐ droit d'opposition et droit à la limitation du traitement (articles 18, 19 et 21);
      - ☐ relations avec les sous-traitants (article 28);
      - ☐ garanties entourant le ou les transferts internationaux (chapitre V);
      - ☐ consultation préalable (article 36);
- ☐ les risques pour les droits et libertés des personnes concernées sont gérés [article 35, paragraphe 7, point c)]:
  - ☐ l'origine, la nature, la particularité et la gravité des risques sont évalués (considérant 84) ou, plus spécifiquement, pour chaque risque (accès illégitime aux données, modification non désirée des données, disparition des données) du point de vue des personnes concernées:
    - ☐ les sources de risques sont prises en compte (considérant 90);
    - ☐ les impacts potentiels sur les droits et libertés des personnes concernées sont identifiés en cas d'événements tels qu'un accès illégitime aux données, une modification non désirée de celles-ci 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 sont identifiées;
    - ☐ la probabilité et la gravité sont évaluées (considérant 90);
  - ☐ les mesures envisagées pour faire face à ces risques sont déterminées [article 35, paragraphe 7, point d), et considérant 90];
- ☐ les parties intéressées sont impliquées:
  - ☐ l'avis du DPD est recueilli (article 35, paragraphe 2);

- ☐ le point de vue des personnes concernées ou de leurs représentants est recueilli, le cas échéant (article 35, paragraphe 9).