GUIDE AIPD

Le présent document a pour ambition de servir de guide pour déterminer si oui ou non une analyse d'impact relative à la protection des données (AIPD) doit être réalisée préalablement à la mise en place d'un traitement envisagé.

Il ne concerne pas les responsables de traitements soumis au respect des titres 2 et 3 de la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel (des autorités judiciaires, des services de police, de l'Inspection générale de la police fédérale et de la police locale, de la Cellule de Traitement des Informations Financières, de l'Administration générale des douanes et accises, et de l'Unité d'information des passagers, services de renseignements et de sécurité,…).

Si vous arrivez à la conclusion que vous devez réaliser un AIPD pour votre projet de traitement à haut risque et que vous disposez d'un délégué à la protection des données, vous êtes tenu de solliciter son avis à ce sujet et de l'associer à sa réalisation. Cet avis sera intégré dans votre documentation interne concernant votre traitement à haut risque.

Si votre projet de traitement de données à haut risque résiduel présente un caractère transfrontalier, vous devrez répondre aux questions a à g et 26 du formulaire afin de déterminer si l'APD belge est l'autorité compétente pour rendre un avis sur votre projet de traitement.

Dans le présent guide, est également abordée la question de savoir quand les responsables de traitement doivent solliciter l'avis d'une Autorité de Protection des données (APD) sur le traitement concerné.

Pour de plus amples précisions, il convient de consulter les lignes directrices du groupe de travail «article 29 » sur la protection des données (Groupe 29) concernant l'AIPD et la manière de déterminer si un traitement est susceptible d'engendrer un risque élevé aux fins du RGPD adoptées le 4 octobre 2017 (WP 248 rév. 01)[1] ainsi que la Recommandation d'initiative de la Commission de protection de la vie privée (CPVP) 01/2018 du 28 février 2018 concernant l'analyse d'impact à la protection des données et la consultation préalable[2].

[1] Disponible à l'adresse suivante : https://www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents/wp248%20rev.01_fr.pdf
[2] Disponible à l'adresse suivante : https://www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents/recommandation_01_2018.pdf

1. DOIS-JE REALISER UNE ANALYSE D'IMPACT A LA PROTECTION DES DONNEES AVANT DE METTRE EN PLACE MON TRAITEMENT DE DONNEES?

L'article 35.1 du RGPD impose à tout responsable de traitement qui envisage de procéder à un traitement susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques de procéder à l'analyse d'impact à la protection des données du traitement envisagé.

Cette obligation concerne uniquement les traitements à haut risque et ce seulement s'il s'agit de nouveaux traitements présentant ces caractéristiques à partir du 25/05/2018 ou de traitements existants présentant un changement (modification de technologie, de méthode de collecte de données, d'ampleur de données collectées ou de catégories de données collectées, …) impliquant un niveau de risque élevé pour les droits et libertés des personnes concernées.

Il existe des listes de traitements considérés comme à haut risque ainsi qu'une liste de critères permettant de déterminer le caractère à haut risque d'un traitement.

Les projets de traitement figurant dans l'énumération reprise à l'article 35.3 du RGPD (Point a) ci-dessous) doivent obligatoirement faire l'objet d'une AIPD préalablement à leur réalisation.

Il n'est pas fait mention dans le présent guide du projet de liste des traitements que l'APD a considéré comme étant à haut risque et qui sont repris en annexe 2 de sa Recommandation précitée 01/2018 étant donné que ce projet de liste doit encore faire l'objet d'un avis du Comité européen à la protection des données avant de pouvoir être adopté par l'APD et avoir force obligatoire.

Dans la mesure où le projet de liste de traitements considérés comme n'étant pas à haut risque figurant en annexe 3 de cette Recommandation 01/2018 présente le même statut, il n'en est également pas fait mention dans le présent guide.

Si un traitement en projet ne figure pas dans la liste de traitements visée à l'article 35.3 du RDGD (**point a)** ci-dessous), il devra tout même faire l'objet d'une AIPD préalable s'il rencontre les critères édictés par le Groupe 29 pour déterminer le caractère à haut risque d'un traitement pour les droits et libertés des personnes concernées (**point b)** ci-dessous).

a. Listes des traitements de données à caractère personnel pour lesquels la réalisation d'une AIPD préalable est obligatoire

En vertu de l'article 35.3 du RGPD, si vous envisagez de réaliser un des traitements de données à caractère personnel suivants, vous devez procéder une analyse de leur impact sur les droits et libertés des personnes concernées préalablement à leur mise en place :

- 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 ;

- *traitement à grande échelle de catégories particulières de données à caractère personnel* visées à l'article 9, paragraphe 1, ou de données à caractère personnel relatives à des condamnations pénales et à des infractions visées à l'article 10 ;
- *surveillance systématique à grande échelle d'une zone accessible au public.*[3]

b. Critères aidant à la détermination du caractère à haut risque d'un traitement de données à caractère personnel

Le Groupe 29 a identifié **neuf critères** que les responsables du traitement doivent prendre en considération dans leur analyse du caractère à risque élevé ou non pour les droits et libertés des personnes physiques de leur projet de traitement de données à caractère personnel. Ces critères sont repris dans la liste ci-dessous.

De manière générale, plus le traitement envisagé cumule le nombre de critères, plus il est probable qu'il implique un risque élevé pour les droits et libertés des personnes concernées, et donc qu'il requière une AIPD préalable. Dans la plupart des cas, un responsable du traitement peut partir du principe que si un traitement répond à **deux critères**, une analyse d'impact relative à la protection des données doit être réalisée. Dans certains cas, un responsable du traitement peut toutefois estimer qu'un traitement qui ne répond qu'à un seul de ces critères requiert une analyse d'impact relative à la protection des données.[4]

Les 9 critères sont les suivants :

- 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"[5].

- Prise de décision automatisée avec effet juridique ou effet similaire significatif sur la personne concernée[6].

- Surveillance systématique : ce critère est rempli par des traitements utilisés pour observer, surveiller ou contrôler les personnes concernées, y compris la collecte de données via des réseaux et par la surveillance systématique d'une zone accessible au public. Il s'agit d'un critère de présomption de traitement à haut risque 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

[3] Pour une interprétation des traitements visés dans cette énumération, cf. les considérants 23 à 27 de la Recommandation précitée 01/2018.
[4] Pour des exemples supplémentaires d'application de ces critères, voir Groupe 29, Lignes directrices AIPD, p. 13-14, disponible à l'adresse suivante http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236 .
[5] Voir également les considérants (71), (75) et (91) du RGPD. À titre d'exemples, prenons le cas d'un établissement financier passant ses clients au crible à partir 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.
[6] Pour plus de précisions sur ces notions, il est renvoyé aux lignes directrices du Groupe 29 sur les décisions individuelles automatisées et le profilage au sens du RGPD (WP 251.rev01) disponibles à l'adresse suivante http://ec.europa.eu/newsroom/article29/document.cfm?doc_id=49826

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[7].

- Données sensibles ou données à caractère hautement personnel : ce critère est rempli pour les catégories particulières de données à caractère personnel visées à l'article 9 (données révélant l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, les traitements de données biométriques aux fins d'identifier de manière unique une personne physique, données concernant la santé ou des données concernant la vie sexuelle) et à l'article 10 du RGPD (données à caractère personnel relatives aux condamnations pénales ou aux infractions ou mesures de sûreté connexes) visées à l'article 10. Sont également concernées les données à caractère personnel qui sont considérées de manière générale comme sensibles dans la mesure où elles sont inhérentes à l'activité domestique et privée d'une personne (communications électroniques dont la confidentialité doit être protégée, par exemple), où elles ont un impact sur l'exercice d'un droit fondamental (données de localisation dont la collecte peut influencer la liberté de mouvement, par exemple) ou dans la mesure où leur divulgation aurait clairement des incidences graves dans la vie quotidienne de la personne concernée (données financières susceptibles d'être utilisées pour des paiements frauduleux, par exemple)[8].

- Traitement de données à caractère personnel à grande échelle, compte tenu :
  - du nombre de personnes concernées (soit en valeur absolue, soit en proportion de la population considérée) ;
  - du volume de données et/ou de l'éventail des différents éléments de données traitées ;
  - de la durée ou de la permanence de l'activité de traitement de données ;
  - de l'étendue géographique de l'activité de traitement[9].

- 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[10].

- Données concernant des personnes vulnérables, comme par exemple les enfants, les travailleurs, les personnes souffrant de maladie mentale, les demandeurs d'asile, les personnes âgées, les patients et autres segments les plus vulnérables de la population nécessitant une protection particulière[11]. 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

[7] Pour des exemples d'activités pouvant constituer un suivi régulier et systématique de personnes concernées, il est renvoyé au point 2.1.4 des lignes directrices du Groupe 29 sur le délégué à la protection des données disponible en plusieurs versions linguistiques à l'adresse suivante http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48137

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

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

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

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

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.

- Utilisation ou application innovante de nouvelles solutions technologiques ou organisationnelles, comme l'utilisation combinée de systèmes de reconnaissance des empreintes digitales et de reconnaissance faciale pour améliorer le contrôle des accès physiques, etc. Il s'agit d'un critère parce que l'utilisation de la technologie en question peut impliquer de nouvelles formes de collecte et d'utilisation des données, présentant potentiellement un risque élevé pour les droits et libertés des personnes physiques[12].

- Lorsque, du fait du traitement lui-même, les personnes concernées ne peuvent pas exercer un droit ou bénéficier d'un service ou d'un contrat[13]. Cela comprend les opérations visant à autoriser, modifier ou refuser l'accès des personnes concernées à un service ou la possibilité de ces personnes de conclure un contrat[14].

Enfin, il est possible qu'un responsable du traitement ne considère pas comme "susceptible d'engendrer un risque élevé" un traitement qui correspond pourtant à certains des critères précités. Dans de tels cas, le responsable du traitement doit **motiver et documenter** les raisons pour lesquelles aucune analyse d'impact relative à la protection des données n'a été réalisée et il doit consigner/enregistrer dans cette documentation ainsi que les avis du délégué à la protection des données (s'il dispose d'un tel délégué) y relatifs pour pouvoir les mettre à disposition de l'Autorité de protection des données à première demande

c. Exemption à l'obligation de réaliser une AIPD préalable ?

L'article 35.10 du RGPD exempte certains responsables de traitement de l'obligation de réaliser une AIPD préalable à la mise en place de certains traitements de données à haut risque. Il s'agit des traitements effectués en application de l'article 6.1.c (traitements nécessaires au respect d'une obligation légale à laquelle le responsable du traitement est soumis) ou 6.1.e du RGPD (traitements nécessaires à l'exécution d'une mission de service public ou relevant de l'exercice de l'autorité publique dont est investi le responsable de traitement).

Toutefois, aux termes de l'article 23 de la loi précitée du 30 juillet 2018, le législateur belge a fait usage de la délégation qui lui était offerte par cet article 35.10 du RGPD pour considérer qu'une analyse d'impact spécifique devait tout de même être réalisée par les responsables de traitement concernés même si une analyse d'impact générale relative à la protection des données a déjà été réalisée dans le cadre de l'adoption de la base légale.

[12] Le fait de déterminer si une technologie doit être considérée ou non comme étant "nouvelle" doit se faire "en conformité avec l'état des connaissances technologiques".
[13] Voir l'article 22 et le considérant (91) du RGPD.
[14] À titre d'exemple, prenons le cas d'une banque passant ses clients au crible à partir d'une base de données de cote de crédit avant d'arrêter ses décisions d'octroi de prêt.

2. QUAND DOIS-JE DEMANDER L'AVIS DE L'APD SUR LE PROJET DE TRAITEMENT ENVISAGE ?

Tous les traitements devant obligatoirement faire l'objet d'une AIPD préalable ne doivent pas être soumis à l'avis préalable de l'autorité de protection des données.

Seuls ceux qui présentent encore un **risque résiduel élevé** malgré les mesures de gestion des risques envisagées par le responsable de traitement doivent être soumis à l'avis préalable de l'autorité de protection des données.

L'obligation de consultation préalable de l'APD prévue à l'article 36 du GDPR n'est en effet d'application que pour les traitements de données présentant un haut risque résiduel pour les droits et libertés des personnes concernées. Un traitement présentant un haut risque résiduel signifie qu'il présente un haut risque malgré les mesures envisagées par le responsable de traitement pour atténuer ce risque.

C'est la raison pour laquelle les informations à compléter dans le formulaire de consultation de l'Autorité de protection des données ou ses annexes ne doivent donc porter que sur ce traitement à haut risque résiduel.

3. EN CAS DE PROJET DE TRAITEMENT A HAUT RISQUE RESIDUEL PRESENTANT UN CARACTERE TRANSFRONTALIER, A QUELLE AUTORITE DE PROTECTION DES DONNEES PUIS-JE M'ADRESSER?

L'article 4, §23 du Règlement Général sur la Protection des données définit le traitement transfrontalier comme un traitement de données à caractère personnel :

> « *qui a lieu dans l'Union dans le cadre des activités d'établissements dans plusieurs États membres d'un responsable du traitement ou d'un sous-traitant lorsque le responsable du traitement ou le sous-traitant est établi dans plusieurs États membres ;*
>
> *ou*
>
> *qui a lieu dans l'Union dans le cadre des activités d'un établissement unique d'un responsable du traitement ou d'un sous-traitant, mais qui affecte sensiblement ou est susceptible d'affecter sensiblement des personnes concernées dans plusieurs États membres* ».

Si votre projet de traitement répond à cette définition et que celui-ci présente un risque résiduel élevé, c'est à l'autorité de protection des données chef de file qu'il convient que vous vous adressiez pour solliciter à ce sujet un avis préalable.

Afin de pouvoir déterminer quelle est cette autorité chef de file pour votre situation, il convient de compléter les questions a à g ainsi que la question 26 du formulaire de demande d'avis AIPD.

Sachez que si, sur base des informations communiquées, l'Autorité de protection des données belge conclut à sa qualité d'autorité chef de file pour le traitement concerné, cette désignation ne saurait toutefois être perçue comme définitive ou fixe. En effet, le

cas échéant, cette décision peut ultérieurement être invalidée par le Comité européen de Protection des données, entre autres suite aux objections qui peuvent éventuellement être formulées par d'autres Autorités de Protection sur sa désignation d'Autorité chef de file.

Si tel est le cas, votre formulaire de demande d'avis sur votre traitement à haut risque résiduel pourrait dès lors être communiqué aux autres autorités de protection compétentes de l'Union européenne.