Commission nationale de l'informatique et des libertés

Délibération n° 2018-326 du 11 octobre 2018 portant adoption de lignes directrices sur les analyses d'impact relatives à la protection des données (AIPD) prévues par le règlement général sur la protection des données (RGPD)

NOR : *CNIL1829637X*

La Commission nationale de l'informatique et des libertés,

Vu le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE, notamment ses articles 35 et 36 ;

Vu la loi du 6 janvier 1978 modifiée, notamment son article 11 ;

Adopte les lignes directrices suivantes sur les analyses d'impact relatives à la protection des données :

Le règlement général sur la protection des données (RGPD) promeut le principe de responsabilisation des organismes, dont la mise en œuvre concrète repose notamment sur la réalisation d'analyses d'impact relatives à la protection des données (AIPD ou *Privacy Impact Assessment - PIA*) pour les traitements susceptibles d'engendrer un risque élevé pour les droits et les libertés des personnes.

En propos liminaires, la Commission nationale de l'informatique et des libertés rappelle l'importance des AIPD qui, au-delà de leur caractère obligatoire dans certaines hypothèses et des sanctions encourues en cas de méconnaissance de cette obligation, permettent à chaque responsable de traitement concerné d'identifier les garanties nécessaires afin d'assurer et de démontrer la conformité du traitement qu'il envisage de mettre en œuvre au regard des exigences du RGPD. Les AIPD sont avant tout l'occasion de mener une réflexion interne, spécifique à chaque traitement, de nature à garantir de manière opérationnelle le respect des principes relatifs à la protection des données et de pouvoir, le cas échéant, le démontrer.

La commission a donc souhaité accompagner les responsables de traitement dans cette démarche essentielle en leur proposant différents outils tels que des guides méthodologiques ainsi qu'un logiciel d'aide à la rédaction des AIPD, disponibles sur son site.

En complément de celles adoptées le 4 octobre 2017 au niveau européen par le groupe de travail « article 29 » (G29), et reprises à son compte par le Comité européen à la protection des données (CEPD) le 25 mai 2018, la commission a également estimé utile d'adopter des lignes directrices afin de préciser le périmètre de l'obligation d'effectuer une AIPD, les conditions de réalisation de celle-ci et, enfin, les cas dans lesquels une AIPD doit lui être transmise.

Les responsables de traitement concernés par la réalisation d'une AIPD pourront également se reporter aux référentiels sectoriels que la commission a adoptés afin, d'une part, d'évaluer la nécessité et la proportionnalité des opérations de traitement envisagées ou mises en œuvre et, d'autre part, d'identifier les garanties devant être apportées pour protéger les droits et libertés des personnes dont les données seront traitées. Ces référentiels pourront éclairer utilement les responsables de traitement sur les attentes de la commission.

La commission pourra par ailleurs, dans certains cas, donner à ces référentiels un effet juridique, en exonérant de la réalisation d'AIPD les responsables de traitement qui s'y conformeraient strictement. Chaque référentiel précisera les effets qui lui sont attachés (référentiel servant de simple aide à la rédaction des AIPD ; référentiel permettant d'être exonéré de la réalisation d'une AIPD).

1. Périmètre des traitements soumis, ou non, à la réalisation d'une AIPD

1.1. *Traitements soumis à la réalisation d'une AIPD*

L'article 35.1 du RGPD prévoit que le responsable doit effectuer une AIPD lorsqu'un traitement est susceptible d'engendrer « *un risque élevé pour les droits et libertés des personnes physiques* ».

- **Le règlement lui-même donne trois types de traitements susceptibles de présenter un risque élevé :**
  - l'évaluation systématique et approfondie d'aspects personnels fondée sur un traitement automatisé 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 ;
  - le traitement à grande échelle de données sensibles ou relatives à des condamnations pénales et des infractions ;
  - la surveillance systématique à grande échelle d'une zone accessible au public.
- **Au-delà de ces trois traitements, le CEPD a identifié neuf critères permettant de caractériser un traitement susceptible d'engendrer un risque élevé :**
  - données traitées à grande échelle ;

- données sensibles (origine raciale ou ethnique, opinions politiques, convictions religieuses ou philosophiques, appartenance syndicale, données génétiques ou de santé, données biométriques et données concernant la vie ou l'orientation sexuelle) ou données à caractère hautement personnel (données relatives à des communications électroniques, données de localisation, données financières, etc.) ;
- données concernant des personnes vulnérables (patients, personnes âgées, enfants, etc.) ;
- croisement ou combinaison de données ;
- évaluation/*scoring* (y compris le profilage) ;
- prise de décision automatisée avec un effet juridique ou similaire ;
- surveillance systématique de personnes ;
- traitement pouvant exclure du bénéfice d'un droit, d'un service ou d'un contrat ;
- utilisation innovante ou application de nouvelles solutions technologiques ou organisationnelles.

La commission considère, de manière générale, qu'un traitement qui rencontre au moins deux des critères mentionnés ci-dessus doit faire l'objet d'une AIPD.

Il sera cependant possible de s'écarter de la recommandation ci-dessus dans certains cas de figure. Un responsable qui estime que son traitement, bien que rencontrant deux des critères mentionnés ci-dessus, ne présente en réalité pas de « risque élevé », devrait expliquer et documenter sa décision de ne pas procéder à une AIPD en incluant, s'il a été désigné, l'avis du délégué à la protection des données (DPO). A l'inverse, un responsable peut estimer que son traitement présente un risque élevé bien qu'il ne satisfasse qu'à un seul des critères ci-dessus. En conséquence, il réalisera une AIPD.

La commission estime, qu'en cas de doute, une AIPD devrait être effectuée.

- **Enfin, le RGPD demande aux autorités de contrôle d'établir une liste de traitements pour lesquels une AIPD est requise (article 35.4).**

Cette liste a été établie par la commission dans le cadre de sa délibération n° 2018-327 du 11 octobre 2018 relative aux types d'opérations de traitement pour lesquelles une analyse d'impact relative à la protection des données est requise, après prise en compte de l'avis rendu par le CEPD le 25 septembre 2018 ; cette liste est appelée à être régulièrement revue par la commission selon son appréciation des « risques élevés » que peuvent présenter certains traitements.

1.2. *Traitements non soumis à AIPD*

D'une manière générale, ne sont pas soumis à AIPD les traitements qui ne sont pas susceptibles d'engendrer un « *risque élevé pour les droits et libertés des personnes physiques* ».

- **Le RGPD autorise les autorités nationales de protection des données à adopter une liste d'opérations de traitement qui ne doivent pas être précédées d'une AIPD (article 35.5).**

Sur ce fondement, la commission établira une liste des traitements qui, en tout état de cause, ne présentent pas de risque élevé et ne sont donc pas soumis à la réalisation d'une AIPD. Ici aussi, cette liste sera régulièrement revue par la commission.

- **Sauf disposition légale contraire, ne sont pas non plus soumis à AIPD les traitements répondant au respect d'une obligation légale à laquelle le responsable de traitement est soumis, ou nécessaires à l'exercice d'une mission de service public confié au responsable de traitement, lorsque ces traitements ont une base juridique dans le droit national ou de l'Union européenne, que ce droit les réglemente, et qu'une AIPD a déjà été menée lors de l'adoption de cette base juridique.**

La commission considère que cette possibilité devrait être largement utilisée par les pouvoirs publics, compte tenu de sa portée et de l'aide qu'elle procurera aux responsables de traitement concernés.

- **Une AIPD n'est pas non plus requise lorsque la nature, la portée, le contexte et les finalités des traitements envisagés sont très similaires à un traitement pour lequel une AIPD a déjà été menée par le responsable de traitement ou par un tiers** (autorités ou organismes publics, regroupement de responsables de traitement, etc.) ; dans ce cas, les résultats de l'AIPD déjà menée peuvent être réutilisés.

Toutefois, dans le cas d'une AIPD effectuée par un tiers, le responsable de traitement concerné doit transposer, pour tout ou partie, les résultats de l'AIPD à sa situation particulière.

La commission rappelle que, pour autant, les traitements non soumis à AIPD doivent respecter les principes de protection des données rappelés à l'article 5 du RGPD et les droits des personnes concernées. La commission a élaboré des référentiels sectoriels permettant d'apporter des garanties de nature à assurer la conformité au RGPD auxquels pourront se référer, le cas échéant, les responsables de traitement concernés.

1.3. *Cas particuliers des traitements mis en œuvre avant l'entrée en vigueur du RGPD*

La commission considère que les traitements régulièrement mis en œuvre avant le 25 mai 2018 – c'est-à-dire ayant fait l'objet d'une formalité auprès de la CNIL, en ayant été dispensés, ayant été autorisés par un acte réglementaire ou encore ayant été inscrits dans le registre d'un correspondant « informatique et libertés » (CIL) – n'ont pas à faire l'objet d'une AIPD dans un délai de trois ans à compter du 25 mai 2018, à moins que ceux-ci n'aient fait l'objet d'une modification substantielle depuis leur mise en œuvre.

2. **Conditions de réalisation d'une AIPD**

Une AIPD doit être menée avant la mise en œuvre d'un traitement présentant un risque élevé pour les droits et libertés des personnes physiques concernées ; elle doit être revue de manière régulière, en tout état de cause tous les trois ans, pour s'assurer que le niveau de risque reste acceptable. Une seule et même AIPD peut porter sur un ensemble d'opérations de traitement similaires en termes de nature, périmètre, contexte, finalité et risques présentés pour les droits et libertés des personnes concernées.

L'article 35.7 du RGPD énonce le contenu minimal d'une AIPD :

– une description systématique des opérations de traitement envisagées et de ses finalités
– une évaluation de la nécessité et de la proportionnalité des opérations de traitement au regard des finalités ;
– une évaluation des risques pour les droits et libertés des personnes concernées, et
– les mesures envisagées pour faire face aux risques.

Quelle que soit la méthode choisie par le responsable de traitement, la commission estime que celle-ci doit permettre de satisfaire aux critères dégagés par le CEPD dans ses lignes directrices du 4 octobre 2017 (« critères d'acceptabilité d'une AIPD »).

Une AIPD doit être menée par le responsable du traitement concerné, ou sous son autorité.

La commission rappelle que la réalisation d'une AIPD doit impliquer l'ensemble des acteurs du traitement considéré. Cela concerne, le cas échéant, et de manière non exhaustive :

– le délégué à la protection des données (DPO) dont le conseil doit être demandé et formalisé dans l'AIPD et le responsable de la sécurité des systèmes d'information (RSSI) ;
– le ou les sous-traitants concernés qui ont une obligation de coopération ;
– les personnes concernées par le traitement ou leurs représentants, dont la consultation peut, dans certains cas, être pertinente pour évaluer les risques ;
– la maîtrise d'ouvrage et la maîtrise d'œuvre en fonction du contexte.

La commission recommande de documenter les apports de chaque acteur sollicité ou, à l'inverse, le choix fait de ne pas recueillir l'avis d'un acteur donné.

Enfin, la commission estime qu'un responsable ayant réalisé une AIPD peut utilement produire un rapport ou un résumé ayant vocation à être publié afin de créer un climat de confiance et de transparence entre les parties concernées par un traitement.

3. **Obligations de transmission d'une AIPD à la CNIL**

Une AIPD faisant apparaître des risques résiduels élevés malgré les mesures envisagées par le responsable de traitement concerné doit être transmise à la CNIL dans les conditions prévues par l'article 36 du RGPD.

Le responsable de traitement pourra, le cas échéant, s'appuyer sur les référentiels sectoriels édictés par la CNIL : le respect d'un référentiel permettra de considérer qu'il n'y a pas de risques résiduels élevés tandis que les traitements s'en écartant devront conduire le responsable de traitement concerné a, *a minima*, s'interroger sur le niveau de risque résiduel pouvant nécessiter la consultation obligatoire de la commission.

Enfin, la commission estime qu'une AIPD portant sur un projet de traitement relevant de l'article 54 III de la loi « informatique et libertés » (traitements de données à caractère personnel dans le domaine de la santé) doit lui être transmise dans le cadre de l'instruction de la demande d'autorisation dont elle est saisie.

En tout état de cause, la commission rappelle que les AIPD pourront, en application des articles 58 du RGPD et 44 de la loi du 6 janvier 1978, être demandées aux responsables de traitement concernés, notamment dans le cadre de l'instruction des plaintes dont elle serait saisie ou dans le cadre du contrôle de la mise en œuvre des traitements.

La présidente
I. Falque-Pierrotin