edpb
European Data Protection Board

Avis du comité (article 64)

Avis 9/2018

sur le projet de liste établi par l'autorité de contrôle compétente de la France

concernant

les opérations de traitement pour lesquelles une analyse d'impact relative à la protection des données est requise (article 35, paragraphe 4, du RGPD)

adopté le 25 septembre 2018

Table des matières

Le comité européen de la protection des données,

vu l'article 63, l'article 64, paragraphe 1, point a), l'article 64, paragraphes 3 à 8, et l'article 35, paragraphes 1, 3, 4 et 6, du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (ci-après le «RGPD»),

vu l'accord sur l'Espace économique européen, et notamment son annexe XI et son protocole 37, tels que modifiés par la décision du Comité mixte de l'EEE nº 154/2018 du 6 juillet 2018,

vu les articles 10 et 22 de son règlement intérieur du 25 mai 2018,

considérant ce qui suit:

(1) La mission principale du comité est de veiller à l'application cohérente du RGPD dans l'ensemble de l'Espace économique européen. Conformément à l'article 64, paragraphe 1, du RGPD, le comité doit émettre un avis chaque fois qu'une autorité de contrôle envisage d'adopter une liste d'opérations de traitement pour lesquelles une analyse d'impact relative à la protection des données doit être effectuée en application de l'article 35, paragraphe 4, du RGPD. L'objectif du présent avis est dès lors de mettre au point une approche harmonisée concernant les activités de traitement qui sont transfrontalières ou qui peuvent affecter la libre circulation des données à caractère personnel ou des personnes physiques au sein de l'Union européenne. Bien que le RGPD n'impose pas de liste unique, il encourage la cohérence. Le comité poursuit cet objectif de cohérence dans ses avis, premièrement en demandant aux autorités de contrôle d'inclure certains types de traitement dans leurs listes, deuxièmement en leur demandant de supprimer certains critères qui, selon lui, n'engendrent pas nécessairement des risques élevés pour les personnes concernées, et troisièmement en leur demandant d'utiliser certains critères de manière harmonisée.

(2) Conformément à l'article 35, paragraphes 4 et 6, du RGPD, les autorités de contrôle compétentes doivent établir des listes des types d'opérations de traitement pour lesquelles une analyse d'impact relative à la protection des données (ci-après l'«AIPD») est requise. Elles doivent cependant appliquer le mécanisme de contrôle de la cohérence lorsque ces listes comprennent des opérations 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.

(3) Si les projets de liste des autorités de contrôle compétentes sont soumis au mécanisme de contrôle de la cohérence, cela ne signifie pas pour autant que ces listes doivent être identiques. Les autorités de contrôle compétentes disposent d'une marge d'appréciation en

ce qui concerne le contexte national ou régional et doivent tenir compte de leur législation locale. L'objectif de l'évaluation/avis du comité européen de la protection des données (ci-après l'«EDPB») n'est pas d'établir une liste unique pour l'Union, mais plutôt d'éviter les incohérences significatives qui pourraient porter atteinte à la protection équivalente des personnes concernées.

(4) Conformément à l'article 35, paragraphe 1, du RGPD, la réalisation d'une AIPD par le responsable du traitement n'est obligatoire que lorsque le traitement «est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques». L'article 35, paragraphe 3, du RGPD contient des exemples de cas susceptibles d'engendrer un risque élevé. Cette liste n'est pas exhaustive. Dans ses lignes directrices concernant l'analyse d'impact relative à la protection des données[1], telles qu'approuvées par l'EDPB[2], le groupe de travail «Article 29» a défini des critères permettant de déterminer les opérations de traitement pour lesquelles une AIPD est obligatoire. Selon les lignes directrices WP 248 du groupe de travail «Article 29», dans la plupart des cas, le responsable du traitement peut considérer qu'un traitement satisfaisant à deux critères nécessite une AIPD; 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.

(5) Les listes élaborées par les autorités de contrôle compétentes visent le même objectif, à savoir déterminer les opérations de traitement qui sont susceptibles d'engendrer un risque élevé et qui, dès lors, requièrent une AIPD. Par conséquent, il convient d'appliquer les critères établis dans les lignes directrices du groupe de travail «Article 29» au moment d'évaluer si les projets de liste des autorités de contrôle compétentes ne portent pas atteinte à une application cohérente du RGPD.

(6) Vingt-deux autorités de contrôle compétentes ont soumis leurs projets de liste à l'EDPB. Une évaluation globale de ces projets de liste soutient l'objectif d'application cohérente du RGPD en dépit de la complexité croissante de la question.

(7) L'avis de l'EDPB doit être adopté conformément à l'article 64, paragraphe 3, du RGPD, en liaison avec l'article 10, paragraphe 2, du règlement intérieur de l'EDPB, dans un délai de huit semaines à compter du premier jour ouvrable après que le président du comité et l'autorité de contrôle compétente ont décidé que le dossier était complet. Sur décision du président, ce délai peut être prolongé de six semaines en fonction de la complexité de la question,

A ADOPTÉ LE PRÉSENT AVIS:

[1] Groupe de travail «Article 29», lignes directrices concernant l'analyse d'impact relative à la protection des données (AIPD) et la manière de déterminer si le traitement est «susceptible d'engendrer un risque élevé» aux fins du règlement (UE) 2016/679 (WP 248 rév. 01).

[2] EDPB, *Endorsement 1/2018*.

1. Résumé des faits

La Commission nationale de l'informatique et des libertés (ci-après l'«autorité de contrôle française») a soumis son projet de liste à l'EDPB. La décision relative au caractère complet du dossier a été prise le 9 juillet. La période au terme de laquelle l'avis devait être adopté a été prolongée jusqu'au 25 septembre compte tenu de la complexité de la question, étant donné que vingt-deux autorités de contrôle compétentes avaient soumis leurs projets de liste en même temps, rendant une évaluation globale nécessaire.

2. Évaluation

2.1 Raisonnement général de l'EDPB concernant la liste soumise

Toute liste soumise à l'EDPB a été interprétée comme précisant davantage l'article 35, paragraphe 1, qui prévaut en tout état de cause. Dès lors, aucune liste ne saurait être exhaustive. Étant donné que ce n'est pas expressément spécifié dans la liste soumise par l'autorité de contrôle française, le comité demande qu'une explication en ce sens soit ajoutée dans le document contenant la liste.

Conformément à l'article 35, paragraphe 10, du RGPD, le comité estime que, si une AIPD a déjà été effectuée dans le cadre d'une analyse d'impact générale réalisée dans le cadre de l'adoption de la base juridique, l'obligation de procéder à une AIPD au titre de l'article 35, paragraphes 1 à 7, du RGPD ne s'applique pas, à moins que l'État membre n'estime qu'une telle AIPD est nécessaire.

En outre, si le comité demande une AIPD pour une certaine catégorie de traitement et qu'une mesure équivalente est déjà requise par la législation nationale, il y a lieu que l'autorité de contrôle française ajoute une référence à cette mesure.

Le présent avis ne porte pas sur les éléments soumis par l'autorité de contrôle française qui ont été considérés comme ne relevant pas du champ d'application de l'article 35, paragraphe 6, du RGPD, à savoir les éléments qui ne sont pas liés «à l'offre de biens ou de services à des personnes concernées» dans plusieurs États membres ni au suivi de leur comportement dans plusieurs États membres et qui ne sont pas non plus susceptibles d'«affecter sensiblement la libre circulation des données à caractère personnel au sein de l'Union». Il s'agit avant tout d'éléments liés à la législation nationale, en particulier lorsque l'obligation de réaliser une AIPD est prévue par celle-ci. En outre, toute opération de traitement liée au domaine répressif a été considérée comme hors cadre, puisqu'elle ne relève pas du champ d'application du RGPD.

Le comité a remarqué que plusieurs autorités de contrôle ont inclus dans leurs listes certains types de traitement qui sont nécessairement des traitements locaux. Étant donné que seuls les traitements transfrontaliers et les traitements susceptibles d'affecter la libre circulation des données à caractère personnel et des personnes concernées sont visés par l'article 35, paragraphe 6, le comité ne s'exprimera pas sur ces traitements locaux.

Le présent avis a pour objectif de définir une base cohérente d'opérations de traitement récurrentes dans les listes fournies par les autorités de contrôle.

Ainsi, pour un nombre limité de types d'opérations de traitement, qui seront définis de manière harmonisée, toutes les autorités de contrôle exigeront la réalisation d'une AIPD, et le comité recommandera à ces autorités de modifier leurs listes en conséquence afin de garantir la cohérence.

Si certaines entrées de la liste soumise ne font l'objet d'aucun commentaire dans le présent avis, cela signifie que l'autorité de contrôle française ne doit rien faire de plus à leur égard.

Enfin, le comité rappelle que la transparence est essentielle pour les responsables du traitement et les sous-traitants. Afin de clarifier les entrées des listes, le comité estime que l'ajout dans ces dernières d'une référence explicite aux critères définis dans les lignes directrices, pour chaque type de traitement, pourrait renforcer cette transparence. Dès lors, le comité considère qu'une explication relative aux critères pris en considération par l'autorité de contrôle française pour élaborer sa liste pourrait être ajoutée.

2.2 Application du mécanisme de contrôle de la cohérence au projet de liste

Le projet de liste soumis par l'autorité de contrôle française est lié à l'offre de biens ou de services à des personnes concernées et au suivi de leur comportement dans plusieurs États membres et/ou peut affecter sensiblement la libre circulation des données à caractère personnel au sein de l'Union, principalement parce que les opérations de traitement qui y figurent ne sont pas limitées aux personnes concernées du pays en question.

2.3 Analyse du projet de liste

Compte tenu du fait que:

a. l'article 35, paragraphe 1, du RGPD requiert une AIPD lorsque l'activité de traitement est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques; et que
b. l'article 35, paragraphe 3, du RGPD contient une liste non exhaustive de types de traitement pour lesquels une AIPD est requise,

le comité émet les observations suivantes.

NATURE INDICATIVE DE LA LISTE

Étant donné que le caractère non exhaustif de la liste n'est pas expressément spécifié dans la liste soumise par l'autorité de contrôle française, le comité demande l'ajout d'une explication en ce sens dans le document contenant la liste.

REFERENCE AUX LIGNES DIRECTRICES

Le comité estime que l'analyse effectuée par le groupe de travail «Article 29» dans ses lignes directrices WP 248 est un élément clé pour garantir la cohérence dans l'ensemble de l'Union. Dès lors, il demande aux différentes autorités de contrôle d'ajouter dans le document

contenant leur liste une mention indiquant que celle-ci est fondée sur ces lignes directrices et qu'elle les complète et les précise davantage.

Étant donné que le document de l'autorité de contrôle française ne contient pas de mention à cet effet, le comité recommande à cette autorité de le modifier en conséquence.

DONNEES BIOMETRIQUES

La liste soumise au comité pour avis par l'autorité de contrôle française prévoit que le traitement de données biométriques en soi relève de l'obligation de réaliser une AIPD. Le comité estime que le traitement de données biométriques en soi n'est pas nécessairement susceptible de présenter un risque élevé. Néanmoins, le traitement de données biométriques effectué aux fins d'identifier une personne physique de manière unique, associé à au moins un autre critère, nécessite la réalisation d'une AIPD. Dès lors, le comité demande à l'autorité de contrôle française de modifier sa liste en conséquence, en ajoutant que l'élément relatif au traitement de données biométriques effectué aux fins d'identifier une personne physique de manière unique requiert une AIPD uniquement lorsqu'il est associé à au moins un autre critère, sans préjudice de l'article 35, paragraphe 3, du RGPD.

DONNEES GENETIQUES

La liste soumise au comité pour avis par l'autorité de contrôle française prévoit que le traitement de données génétiques en soi relève de l'obligation de réaliser une AIPD. Le comité estime que le traitement de données génétiques en soi n'est pas nécessairement susceptible de présenter un risque élevé. Néanmoins, le traitement de données génétiques associé à au moins un autre critère nécessite la réalisation d'une AIPD. Dès lors, le comité demande à l'autorité de contrôle française de modifier sa liste en conséquence, en ajoutant que l'élément relatif au traitement de données génétiques requiert une AIPD uniquement lorsqu'il est associé à au moins un autre critère, sans préjudice de l'article 35, paragraphe 3, du RGPD.

DONNEES DE LOCALISATION

Le comité est d'avis que la cohérence est l'un des principes de base du RGPD. Il constate que, dans leur majorité, les listes soumises font expressément référence au traitement de données de localisation. Étant donné que la liste soumise pour avis par l'autorité de contrôle française ne contient pas de telle référence, le comité encourage cette autorité à inclure le traitement de données de localisation dans sa liste, en association avec un autre critère.

SURVEILLANCE DES EMPLOYES

Le comité est d'avis qu'en raison de sa nature spécifique, le traitement dans le cadre de la surveillance des employés, qui remplit les critères relatifs aux personnes concernées vulnérables et à la surveillance systématique mentionnés dans les lignes directrices, pourrait nécessiter une AIPD. Étant donné que la liste soumise au comité pour avis par l'autorité de contrôle française envisage déjà ce type de traitement comme requérant une AIPD, le comité recommande seulement d'ajouter une référence explicite aux deux critères des lignes directrices WP 248 du groupe de travail «Article 29». En outre, le comité estime que le

document WP 249 du groupe de travail «Article 29» reste valable pour ce qui est de définir la notion de traitement systématique de données d'employés.

3. Conclusions/recommandations

Le projet de liste de l'autorité de contrôle française pourrait entraîner une application incohérente de l'exigence relative à la réalisation d'une AIPD, et les modifications suivantes doivent y être apportées:

- en ce qui concerne la nature indicative de la liste: le comité demande l'ajout, dans le document contenant la liste, d'une explication précisant que celle-ci n'est pas exhaustive;
- en ce qui concerne la référence aux lignes directrices: le comité recommande à l'autorité de contrôle française de modifier son document en conséquence;
- en ce qui concerne les données biométriques: le comité demande à l'autorité de contrôle française de modifier sa liste en ajoutant que l'élément relatif au traitement de données biométriques effectué aux fins d'identifier une personne physique de manière unique requiert une AIPD uniquement lorsqu'il est associé à au moins un autre critère;
- en ce qui concerne les données génétiques: le comité demande à l'autorité de contrôle française de modifier sa liste en ajoutant que l'élément relatif au traitement de données génétiques requiert une AIPD uniquement lorsqu'il est associé à au moins un autre critère;
- en ce qui concerne les données de localisation: le comité encourage l'autorité de contrôle française à inclure le traitement de données de localisation dans sa liste, en association avec un autre critère;
- en ce qui concerne la surveillance des employés: le comité recommande seulement de faire expressément référence aux deux critères des lignes directrices WP 248 du groupe de travail «Article 29».

4. Remarques finales

Le présent avis est adressé à la Commission nationale de l'informatique et des libertés (autorité de contrôle française) et sera publié conformément à l'article 64, paragraphe 5, point b), du RGPD.

Conformément à l'article 64, paragraphes 7 et 8, du RGPD, l'autorité de contrôle doit faire savoir au président du comité par voie électronique, dans un délai de deux semaines suivant la réception de l'avis, si elle modifiera ou si elle maintiendra son projet de liste. Dans le même délai, elle doit fournir son projet de liste modifié ou, si elle n'a pas l'intention de suivre l'avis du comité, en tout ou en partie, elle doit fournir les motifs pertinents justifiant ce choix.

Pour le comité européen de la protection des données

La présidente

(Andrea Jelinek)