



Recommandation n° 02/2019 du 18 octobre 2019

Objet : article 20 de la loi du 30 juillet 2018 *relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel* et protocoles généraux (CO-AR-2019-003)

L'Autorité de protection des données (ci-après "l'Autorité") ;

Vu la loi du 3 décembre 2017 *portant création de l'Autorité de protection des données*, en particulier l'article 23 (ci-après "la LCA") ;

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* (Règlement général sur la protection des données, ci-après "le RGPD") ;

Vu la loi du 30 juillet 2018 *relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel* (ci-après "la LTD") ;

Vu le rapport de Madame Alexandra Jaspar, Directrice du Centre de Connaissances de l'Autorité de protection des données ;

Émet, le 18/10/2019, la recommandation suivante :

I. CONTEXTE

1. L'Autorité a reçu une demande conjointe de l'ASBL Vlaamse Vereniging van Steden en Gemeenten (Union flamande des villes et communes, ci-après la VVSG) et de l'ASBL Onderwijsvereniging van Steden en Gemeenten (association d'enseignement des villes et communes, ci-après l'OVSG).

2. Les villes et communes ont un ensemble de tâches réglementaires identique. Cela s'applique également aux écoles urbaines et communales. Afin d'assurer leurs tâches, il est dans certains cas utile, voire nécessaire, de pouvoir disposer de données à caractère personnel qui sont en possession d'autorités fédérales. Cela nécessite la conclusion d'un protocole entre le responsable du traitement fournisseur et le responsable du traitement destinataire, conformément à l'article 20 de la LTD. Cela signifierait concrètement, par exemple, que lorsque des communes ont besoin d'informations fiscales en vue d'une tâche réglementaire, chaque commune flamande (et il y en a plus de 300) devrait négocier et conclure un protocole avec le SPF Finances. Idem dito pour les écoles communales. Pour le responsable du traitement fournisseur, cela représente une charge de travail non négligeable étant donné qu'il doit se concerter avec chaque commune séparément.

3. La VVSG et l'OVSG ont élaboré une procédure en vue de mettre en place des protocoles généraux. De tels protocoles présentent l'avantage que d'une part, le responsable du traitement fournisseur n'est confronté qu'à un seul interlocuteur et d'autre part, que les modalités d'obtention des données sont les mêmes pour tous les responsables du traitement destinataires du groupe cible.

4. La VVSG et l'OVSG veulent savoir si l'Autorité peut valider une telle initiative. Elles souhaitent également savoir si l'Autorité pense qu'il est possible de conclure des protocoles de cette manière avec des instances fédérales.

5. L'Autorité constate que cette problématique n'est pas propre aux communes et aux écoles communales mais qu'elle est valable pour toutes les instances qui accomplissent des tâches qui sont en grande partie identiques. C'est pourquoi l'Autorité juge utile d'exprimer sa vision de cette problématique par voie de recommandation.

II. ANALYSE

A. Généralités

6. L'Autorité présume que l'idée de conclure des protocoles "généraux" est inspirée des délibérations des comités sectoriels qui octroyaient des autorisations "générales". Les instances qui faisaient partie du groupe cible visé par de telles délibérations (par exemple le groupe cible "communes", le groupe cible "hôpitaux") pouvaient, sous certaines conditions, demander à adhérer à cette délibération. L'acceptation de cette demande d'adhésion valait permission d'utiliser l'autorisation.

7. L'Autorité n'a en principe pas d'objection à la conclusion de protocoles "types". La question qui se pose est de savoir si c'est possible légalement et dans l'affirmative, à quelles conditions.

8. Le protocole évoqué par l'article 20 de la LTD est une convention qui est conclue entre le responsable du traitement qui fournit les données et le responsable du traitement qui reçoit les données. L'article 20, § 1 de la LTD vise la conclusion d'un protocole "individuel" entre 2 responsables du traitement.

9. L'article 20, § 2 de la LTD semble le confirmer. En vertu de cette disposition, un protocole ne peut être conclu qu'après avis à la fois du délégué à la protection des données (ci-après DPO) du fournisseur des données et du DPO du destinataire des données. Ces avis sont annexés au protocole. Si un des avis n'est pas suivi, les motifs en sont repris dans le protocole.

10. Cela signifie-t-il que des protocoles "généraux" soient exclus ? L'Autorité estime que si on se base simplement sur la formulation de l'article 20 de la LTD, des protocoles "généraux" ne sont pas exclus, pour autant qu'ils soient conclus dans le respect des exigences légales mentionnées à l'article 20, §§ 2 et 3 de la LTD.

B. En pratique

B.1. Résolution par des protocoles "types"

11. Avant de se pencher sur la problématique d'un protocole "général", on examine si le problème visé au point 2 ne peut pas malgré tout être résolu en grande partie en concluant des protocoles "individuels" sur la base d'un protocole "type".

12. Lors d'une demande d'un responsable du traitement destinataire, le responsable du traitement fournisseur conclut un protocole concernant une ou plusieurs finalités, pour un ou plusieurs traitements de données. Lorsqu'ensuite d'autres responsables du traitement destinataires se manifestent avec un statut identique ou similaire et souhaitent conclure un protocole pour la ou les mêmes finalités avec les mêmes données, le responsable du traitement fournisseur peut convertir le protocole initial en protocole "type", au sujet duquel son DPO rend un avis, et qu'il met ensuite à la disposition des responsables du traitement intéressés. Une alternative consiste à ce qu'après concertation avec un représentant d'un groupe de responsables du traitement destinataires ou de quelques-uns d'entre eux, le responsable du traitement fournisseur établisse un protocole "type" qu'il met ensuite à disposition des responsables du traitement intéressés, après avis de son DPO. Les deux solutions respectent parfaitement l'article 20, §§ 2 et 3 de la LTD.

13. Un responsable du traitement destinataire concerné peut alors :

- vérifier dans quelle mesure le respect des modalités mentionnées dans le protocole est ou non réalisable pour lui ;
- demander l'avis de son DPO, comme requis par l'article 20, § 2 de la LTD et par l'article 39.1.a) du RGPD.

14. Si les dispositions du protocole "type" ne posent pas de problème pour un responsable du traitement destinataire et que l'avis de son DPO est positif ou du moins pas suffisamment défavorable, le protocole "type" peut être signé en mentionnant les motifs pour lesquels l'avis du DPO n'a pas été suivi, pour autant que ce dernier ait formulé des objections.

15. Cette approche présente l'avantage que :

- un nombre non négligeable de responsables du traitement destinataires peut conclure et signer le protocole "type" ;
- chaque responsable du traitement destinataire est lui-même obligé d'évaluer toutes les modalités du protocole "type", de manière à savoir clairement ce à quoi il s'engage avant de signer.

16. Le fait que le responsable du traitement fournisseur propose un protocole "type" ne signifie pas que ce soit à prendre ou à laisser. Le fait d'appartenir à un groupe de responsables du traitement destinataires ayant un statut similaire n'exclut pas des particularités spécifiques propres à un responsable du traitement déterminé.

17. Si par exemple suite à l'avis de son DPO, le responsable du traitement destinataire constate que certaines modalités du protocole "type" sont problématiques, il peut proposer des adaptations –

qui porteront en principe sur un nombre limité d'éléments du protocole – au responsable du traitement fournisseur. Si ce dernier marque son accord sur les adaptations proposées, le protocole adapté peut être finalisé conformément à l'article 20, §§ 2 et 3 de la LTD (de nouveau après avis des DPO concernés).

18. Étant donné que l'on ne devra adapter que les éléments du protocole qui requièrent une correction en fonction des particularités spécifiques du responsable du traitement destinataire, cela permettra généralement un traitement rapide. À nouveau, les responsables du traitement concernés ne subissent pas le processus passivement. Ils y participent volontairement, ce qui est positif à la lumière du principe de responsabilité de l'article 5.2 du RGPD.

19. À défaut d'un accord sur les adaptations proposées, le cas peut être soumis à la Chambre autorité fédérale du Comité de sécurité de l'information, en application de l'article 35/1, § 1 de la loi du 12 août 2012 *relative à la création et à l'organisation d'un intégrateur de services fédéral*, qui le traitera par voie de délibération qui établira les conditions auxquelles le transfert de données peut intervenir.

20. Cela signifie que le traitement sera un peu plus long, mais il débouchera sur une décision adaptée aux besoins des deux parties concernées.

21. En conclusion, on peut affirmer que la situation où le responsable du traitement fournisseur choisit dans certains cas de mettre un protocole "type" à disposition d'un groupe spécifique de responsables du traitement destinataires est parfaitement conciliable avec l'article 20, §§ 2 et 3 de la LTD. On garantit ainsi un traitement efficace de transferts de données qui ne se fait pas au détriment de l'implication de tous les responsables du traitement. Cette approche n'exclut pas des corrections ponctuelles ni un protocole "type" adapté selon les particularités spécifiques d'un responsable du traitement déterminé. Selon que l'on parvienne ou non à un accord sur les adaptations, l'investissement en temps et en moyens sera un peu plus important.

B.2. Résolution par des protocoles "généraux"

1. L'accord de principe du responsable du traitement fournisseur est requis

22. Comme déjà indiqué au point 8, un protocole est en soi une convention. En cas de protocole "général", cela signifie que le responsable du traitement fournisseur concerné accepte de ne pas régler le transfert de données à un groupe de responsables du traitement destinataires similaires par des protocoles "individuels" mais par un protocole "général". Lorsque par exemple une association demande pour ses membres à un responsable du traitement fournisseur s'il est disposé à régler l'échange de données par un protocole "général", le responsable du traitement fournisseur n'est pas

obligé d'y donner suite. Si le responsable du traitement fournisseur souhaite se concerter séparément avec chacun des responsables du traitement destinataires pour régler les modalités du transfert de données, c'est son droit le plus strict.

2. Le protocole "général", de facto une variante du protocole "type" ?

23. Un protocole "général" suppose qu'une personne/organisation élabore, au nom d'un groupe de responsables du traitement destinataires, un règlement avec le responsable du traitement fournisseur. Cette personne/organisation doit être dûment mandatée à cet effet et se pose alors la question de la portée de ce mandat : implique-t-il uniquement l'élaboration d'un protocole ou comprend-il également la conclusion du protocole.

24. L'Autorité estime que le mandat doit être limité à la négociation des modalités du protocole avec le responsable du traitement fournisseur, donc la mise au point d'un texte qui, après avis du DPO du responsable du traitement fournisseur, est remis à tous les responsables du traitement destinataires concernés pour finalisation, comme prévu par l'article 20, § 2 de la LTD. Lors de la mise au point du protocole, le responsable du traitement fournisseur n'a qu'un seul interlocuteur, ce qui facilite les choses mais la conclusion finale doit bien avoir lieu en "one-on-one".

25. Concrètement, cela signifie en réalité qu'à partir de ce stade, on suit les mêmes parcours que pour la solution du protocole "type", telle qu'exposée aux points 13 à 20.

26. Cela rejoint d'ailleurs l'article 5.2 du RGPD qui met en avant le principe de responsabilité du responsable du traitement. Cela signifie que la responsabilité du respect du RGPD incombe uniquement au responsable du traitement étant donné qu'il prend la décision relative au traitement. Il s'agit d'une responsabilité qu'il ne peut reporter sur personne d'autre, ni *de jure*, ni *de facto*. Il en résulte que le responsable du traitement doit documenter ses décisions relatives au traitement de données à caractère personnel afin de pouvoir démontrer la conformité de ses actes avec le RGPD.

27. Les points 24 et 25 illustrent qu'un mandat qui va plus loin, donc jusqu'à la conclusion du protocole, a peu de sens vu l'absence de toute plus-value. Dans l'hypothèse où un mandataire pourrait conclure et signer un protocole pour les responsables du traitement destinataires, cela signifierait à la lumière de l'article 5.2 du RGPD que le mandat devrait être très détaillé. Dès que le protocole "général" contient des dispositions qui s'écartent du mandat ou que ce dernier ne couvre pas, le mandataire ne pourra pas signer et l'on retombe sur le parcours dont il est question ci-dessus au point 25.

28. La question se pose de savoir si un tel mandat uniforme et détaillé pour un groupe important de responsables du traitement destinataires est réalisable. Il est très probable qu'ils aient des opinions différentes sur un certain nombre de points régis par un protocole. Pour éviter ce problème, le futur

mandataire pourrait proposer une sorte de mandat standard. Les responsables du traitement destinataires qui donnent un mandat de cette manière doivent être bien conscients du fait qu'au final, ce sont eux qui seront responsables de la conformité avec le RGPD, et pas le mandataire. En tout état de cause, un mandat standard ne permettra pas d'éviter le problème mentionné au point 27.

29. Il existe une exigence non négligeable qui ne peut être ignorée, quelle que soit la portée du mandat : en vertu de l'article 20, § 2 de la LTD, le DPO du responsable du traitement destinataire ne peut pas être mis à l'écart. Son avis préalable à la conclusion du protocole est obligatoire. Il doit pouvoir exercer sa fonction d'avis en toute indépendance. Cela signifie qu'il ne peut être mis sous pression ni se sentir sous pression pour valider le protocole soumis sans émettre de critique ("cela ne pose de problème à personne", "c'est quand même facile", ...).

30. Dès que le DPO d'un responsable du traitement destinataire formule une remarque, le mandataire ne peut plus rien faire. Il appartient alors au responsable du traitement concerné de décider des étapes ultérieures : ignorer les remarques et signer malgré tout ; entamer une discussion avec le responsable du traitement fournisseur en vue d'adapter le protocole ; à défaut d'un accord, soumettre l'affaire à la Chambre autorité fédérale du Comité de sécurité de l'information.

B.3. Publicité

31. Le protocole conclu est publié sur le site Internet des responsables du traitement fournisseurs et destinataires. Le but est de garantir une large visibilité¹. Il s'agit d'un élément de transparence important à l'égard de la personne concernée. Pour le responsable du traitement fournisseur et un responsable du traitement destinataire, il s'agit d'un élément illustrant leur responsabilité. À la lumière de cette situation, l'Autorité déconseille que les responsables du traitement concernés se limitent à reprendre un lien vers le site Internet d'un mandataire regroupant les protocoles du groupe cible. Il arrive trop souvent que de tels liens ne soient pas actualisés et qu'en conséquence, les protocoles ne puissent plus être consultés.

PAR CES MOTIFS, l'Autorité,

attire l'attention sur le fait que, conformément au principe de responsabilité (« accountability » - article 5.2 du RGPD), un responsable du traitement ne peut pas se déresponsabiliser, quel que soit le protocole conclu.

¹ Chambre, DOC 54-3126/001, p. 46.

option 1 : un protocole "type"

- le responsable du traitement fournisseur peut, après avis de son DPO, mettre un protocole "type" à disposition d'un groupe cible de responsables du traitement destinataires ;
- un responsable du traitement intéressé recueille l'avis de son DPO ;
- publication effective du protocole/de la délibération sur le propre site Internet des responsables du traitement concernés (pas par le biais de liens vers d'autres sites Internet) ;

option 2 : un protocole "général"

- le responsable du traitement fournisseur n'est pas obligé d'accéder à une proposition de rédiger un protocole "général" ;
- le mandat de la personne/de l'organisation qui agit au nom du groupe cible de responsables du traitement destinataires est limité à l'élaboration d'un protocole "général" ;
- ce protocole "général" est mis à disposition d'un groupe cible de responsables du traitement destinataires, après avis du DPO du responsable du traitement fournisseur ;
- le responsable du traitement destinataire recueille l'avis de son DPO ;
- publication effective du protocole/de la délibération sur le propre site Internet des responsables du traitement concernés (pas par le biais de liens vers d'autres sites Internet).

(sé) Alexandra Jaspar

Directrice du Centre de Connaissances