Autorité de protection des données
Gegevensbeschermingsautoriteit

Chambre Contentieuse

Décision 54/2022 du 11 avril 2022

Numéro de dossier : DOS-2022-00320

Objet : Violation de l'obligation de notification dans le cadre d'une fuite de données

La Chambre Contentieuse de l'Autorité de protection des données, composée de Monsieur Hielke Hijmans, président, siégeant seul ;

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 "RGPD" ;

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

Vu le règlement d'ordre intérieur tel qu'approuvé par la Chambre des représentants le 20 décembre 2018 et publié au *Moniteur belge* le 15 janvier 2019 ;

Vu les pièces du dossier ;

a pris la décision suivante concernant :

le défendeur : Y, ci-après "le responsable du traitement"

I. Faits et procédure

1. Le 21 février 2022, le Comité de direction de l'Autorité de protection des données (ci-après : "APD") a décidé de saisir le Service d'Inspection en vertu de l'article 63, 1° de la LCA en raison d'une pratique susceptible de donner lieu à une violation des principes fondamentaux de la protection des données à caractère personnel.

   Le Comité de direction a été informé du fait que différentes données à caractère personnel de donneurs de sang étaient consultables publiquement sur le site Internet du responsable du traitement. Le Service d'Inspection est saisi par le Comité de direction afin de cerner l'ampleur de cette fuite de données et de vérifier si les dispositions du RGPD y afférentes ont été respectées par le responsable du traitement.

2. Le 30 mars 2022, l'enquête du Service d'Inspection est clôturée, le rapport est joint au dossier et celui-ci est transmis par l'inspecteur général au président de la Chambre Contentieuse (art. 9, § 1er et § 2 de la LCA).

   Le rapport conclut que :

   1. il est question d'une violation de l'article 33 du RGPD ; et
   2. il n'est pas question d'une violation de l'article 34 du RGPD.

II. Motivation

3. Une violation de données à caractère personnel telle que définie à l'article 4, 12° du RGPD est "*une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données*".

4. Lorsqu'une telle violation de données à caractère personnel se produit, le RGPD impose au responsable du traitement de le notifier à l'autorité de contrôle nationale compétente et, dans certains cas, de communiquer cette violation aux personnes dont les données à caractère personnel sont concernées par cette violation.

5. En ce qui concerne la notification d'une violation de données à caractère personnel à l'autorité de contrôle, la Chambre Contentieuse se réfère à l'article 33 du RGPD qui dispose que "*En cas de violation de données à caractère personnel, le responsable du traitement en notifie la violation en question à l'autorité de contrôle compétente conformément à l'article 55, dans les meilleurs délais et, si possible, 72 heures au plus tard après en avoir pris connaissance, à moins que la violation en question ne soit pas susceptible d'engendrer un risque pour les droits et libertés des personnes physiques. Lorsque la notification à l'autorité de contrôle n'a pas lieu dans les 72 heures, elle est accompagnée des motifs du retard*".

6. Conformément à l'article 34 du RGPD, le responsable du traitement doit dans certains cas non seulement notifier une violation à l'autorité de contrôle, mais aussi la communiquer aux personnes touchées par celle-ci. C'est le cas lorsqu'il est probable qu'une violation implique un risque élevé pour les droits et libertés des personnes physiques.

7. Le seuil pour la communication d'une violation aux personnes concernées est donc plus élevé que celui pour la communication aux autorités de contrôle et donc toutes les violations qui sont notifiées à l'autorité de contrôle ne doivent pas être communiquées aux personnes concernées.

8. La Chambre Contentieuse vérifiera tout d'abord si une violation de données à caractère personnel s'est produite et le cas échéant si celle-ci aurait dû être notifiée à l'APD et/ou aux personnes concernées.

9. Sur la base des pièces du dossier, la Chambre Contentieuse constate que le nom, le prénom et les coordonnées directes de certains donneurs de sang étaient visibles publiquement sur le site Internet du responsable du traitement. De ce fait, des personnes externes pouvaient également consulter ces données. C'est en effet une personne externe qui a informé le responsable du traitement du problème. Il est dès lors question d'une violation de confidentialité, à savoir une communication ou un accès illicite ou involontaire de/à des données à caractère personnel. Les données à caractère personnel en question ont en effet été exposées involontairement pendant une (courte) période à des personnes externes, mettant ainsi en péril la confidentialité.

10. Ensuite, la Chambre Contentieuse vérifie si cette violation de données à caractère personnel aurait dû être notifiée à l'APD et par la suite aussi aux personnes concernées.

11. Comme déjà indiqué ci-dessus, la violation de données à caractère personnel doit être notifiée à l'APD, à moins qu'il soit peu probable que celle-ci engendre un risque pour les droits et libertés des personnes concernées.

12. La Chambre Contentieuse constate que le responsable du traitement a adopté une attitude constructive dans le cadre de la demande du Secrétariat Général de l'APD au sujet de cette violation de données à caractère personnel et y a apporté une réponse claire et complète.

13. Le responsable du traitement affirme que la violation de données à caractère personnel résulte d'une erreur dans l'indexation d'une page sur son site Internet. Le problème a été résolu en moins de deux heures après en avoir pris connaissance et aucun autre problème n'a été constaté à l'égard de la protection des données à caractère personnel. Le responsable du traitement affirme ensuite que la violation de données à caractère personnel était de faible ampleur, celle-ci concernant en effet 17 personnes. Le responsable du traitement explique que les données ne pouvaient être consultées par des tiers que si le nom, le prénom et le lieu du don de sang étaient connus.

14. Vu les éléments qui précèdent, le responsable du traitement a décidé de renoncer à une notification à l'APD et aux personnes concernées car il estimait qu'il n'était pas question d'un risque (élevé) pour les droits et libertés des personnes physiques.

15. La Chambre Contentieuse souligne que dans cette affaire, la violation de données à caractère personnel a été remarquée par une personne externe au responsable du traitement, qui en a ensuite informé ce dernier. Il est ainsi établi que les données à caractère personnel en question étaient consultables par des personnes externes. Il ne peut être exclu que d'autres personnes externes aient également pu consulter ces données à caractère personnel. Il existe donc un risque, bien que limité, concernant les droits et libertés des personnes concernées. Le responsable du traitement aurait dès lors dû adresser une notification à l'APD, conformément à l'article 33 du RGPD.

16. En ce qui concerne la notification aux personnes concernées, la Chambre Contentieuse conclut sur la base de des éléments ci-dessus qu'il n'est pas question d'un risque élevé pour les personnes concernées. Comme déjà indiqué, il s'agit d'un nombre limité de données à caractère personnel d'un nombre limité de personnes concernées qui étaient disponibles pendant une période limitée. La Chambre Contentieuse estime donc qu'une notification aux personnes concernées conformément à l'article 34 du RGPD n'était pas nécessaire.

17. Vu les constatations précitées, la Chambre Contentieuse décide de ne pas procéder à un traitement sur le fond de l'affaire. La Chambre Contentieuse estime qu'il est démontré qu'il **n'est pas question d'une violation de l'article 34 du RGPD**, mais bien d'une **violation de l'article 33 du RGPD**, ce qui justifie en l'occurrence de procéder à la prise d'une décision en vertu de l'article 95, § 1er, 4° de la LCA, plus précisément d'avertir le responsable du traitement pour l'avenir que la non-notification d'une violation de données à caractère personnel impliquant un risque pour les droits et libertés des personnes concernées constitue une violation de l'article 33 du RGPD.

18. La présente décision est une décision *prima facie* prise par la Chambre Contentieuse conformément à l'article 95 de la LCA sur la base de la plainte introduite par le plaignant, dans le cadre de la 'procédure préalable à la décision de fond[1]' et non une décision sur le fond de la Chambre Contentieuse au sens de l'article 100 de la LCA. La Chambre Contentieuse a ainsi décidé, sur la base des articles 58.2. c) et 95, § 1, 4° de la loi du 3 décembre 2017, d'avertir le défendeur que la non-notification de la fuite de données précitée constituait une violation de l'article 33 du RGPD.

19. La présente décision a pour but d'informer le défendeur du fait que celui-ci a commis une violation des dispositions du RGPD et de lui permettre d'encore se conformer aux dispositions précitées.

20. Si toutefois, le défendeur n'est pas d'accord avec le contenu de la présente décision *prima facie* et estime qu'il peut faire valoir des arguments factuels et/ou juridiques qui pourraient conduire à une autre décision, celui-ci peut adresser à la Chambre Contentieuse une demande de traitement sur le

[1] Section 3, Sous-section 2 de la LCA (art. 94 à 97 inclus).

fond de l'affaire via l'adresse e-mail litigationchamber@apd-gba.be, et ce dans le délai de 30 jours après la notification de la présente décision.

21. En cas de poursuite du traitement de l'affaire sur le fond, en vertu des articles 98, 2° et 3° *juncto* l'article 99 de la LCA, la Chambre Contentieuse invitera les parties à introduire leurs conclusions et à joindre au dossier toutes les pièces qu'elles jugent utiles. Le cas échéant, la présente décision est définitivement suspendue.

22. Dans un souci d'exhaustivité, la Chambre Contentieuse souligne qu'un traitement de l'affaire sur le fond peut conduire à l'imposition des mesures mentionnées à l'article 100 de la LCA[2].

23. Enfin, la Chambre Contentieuse attire encore l'attention sur ce qui suit :

    Si une des deux parties souhaite recourir à la possibilité de consulter et de copier le dossier (art. 95, § 2, 3° de la LCA), elle doit s'adresser au secrétariat de la Chambre Contentieuse, de préférence via l'adresse e-mail litigationchamber@apd-gba.be, afin de fixer un rendez-vous. Si une copie du dossier est demandée, les pièces seront si possible transmises par voie électronique ou, à défaut, par courrier ordinaire[3].

III. Publication de la décision

24. Vu l'importance de la transparence concernant le processus décisionnel de la Chambre Contentieuse, la présente décision est publiée sur le site Internet de l'Autorité de protection des données. Toutefois, il n'est pas nécessaire à cette fin que les données d'identification des parties soient directement communiquées.

---

[2] *1° classer la plainte sans suite ;*
2° ordonner le non-lieu ;
3° prononcer la suspension du prononcé ;
4° proposer une transaction ;
5° formuler des avertissements et des réprimandes ;
6° ordonner de se conformer aux demandes de la personne concernée d'exercer ses droits ;
7° ordonner que l'intéressé soit informé du problème de sécurité ;
8° ordonner le gel, la limitation ou l'interdiction temporaire ou définitive du traitement ;
9° ordonner une mise en conformité du traitement ;
10° ordonner la rectification, la restriction ou l'effacement des données et la notification de celles-ci aux récipiendaires des données ;
11° ordonner le retrait de l'agréation des organismes de certification ;
12° donner des astreintes ;
13° donner des amendes administratives ;
14° ordonner la suspension des flux transfrontières de données vers un autre État ou un organisme international ;
15° transmettre le dossier au parquet du Procureur du Roi de Bruxelles, qui l'informe des suites données au dossier;
16° décider au cas par cas de publier ses décisions sur le site internet de l'Autorité de protection des données."

[3] Vu les circonstances exceptionnelles en raison du COVID-19, il n'est PAS possible de venir retirer des documents au secrétariat de la Chambre Contentieuse. De plus, toutes les communications se font en principe par voie électronique.

PAR CES MOTIFS,

la Chambre Contentieuse de l'Autorité de protection des données décide, après délibération :

- en vertu de l'article 58.2.a) du RGPD et de l'article 95, § 1er, 4° de la LCA, **d'avertir** le responsable du traitement pour l'avenir que la non-notification d'une violation de données à caractère personnel impliquant un risque pour les droits et libertés des personnes concernées constitue une violation de l'article 33 du RGPD ;
- d'informer le responsable du traitement, conformément à l'article 95, deuxième alinéa, 3° de la LCA, du fait qu'il peut demander une copie du dossier au greffe de la Chambre Contentieuse, de préférence par e-mail via l'adresse litigationchamber@apd-gba.be.

En vertu de l'article 108, § 1er de la LCA, cette décision peut faire l'objet d'un recours auprès de la Cour des marchés dans un délai de trente jours à compter de sa notification, avec l'Autorité de protection des données en qualité de défenderesse.

Hielke HIJMANS

Président de la Chambre Contentieuse