Autorité de protection des données
Gegevensbeschermingsautoriteit

Chambre Contentieuse

Décision 94/2021 du 13 Août 2021

Numéro de dossier : DOS-2020-01112

Objet : Plainte contre une commune et une employée pour consultation illicite du registre national

La Chambre Contentieuse de l'Autorité de protection des données, constituée 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 le "RGPD") ;

Vu la loi du 3 décembre 2017 *portant création de l'Autorité de protection des données*, ci-après la "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 plaignant :	Mme X , ci-après "la plaignante" ;
le responsable de traitement :	Mme Y, employée de la ville Z ;
	La Ville Z, ci-après « la défenderesse ».

I. Faits et procédure

1. Le 2 mars 2020, la plaignante dépose plainte auprès de l'Autorité de protection des données (ci-après : **l'APD**) contre la Ville Z, ainsi que contre Mme Y, employée administrative au service population de la Ville Z. Les faits concernent une consultation illégale des données à caractère personnel de la plaignante reprises au Registre National.

2. Le Service de Première Ligne a déclaré cette plainte recevable et l'a transmise à la Chambre contentieuse le 9 mars 2020. Le 01 avril 2020 la Chambre Contentieuse a transféré le dossier au Service d'Inspection. Celui-ci a communiqué son rapport à la Chambre Contentieuse en date du 27 octobre 2020.

3. La plaignante explique que le 15 février 2019, Mme Y, future épouse de l'ex-conjoint de la plaignante, se serait rendue au domicile de cette dernière à Charleroi, afin de la narguer devant ses enfants. La plaignante suspectant une consultation abusive des données issues du Registre National par Mme Y, elle s'est adressée à la Ville Z auprès de laquelle elle s'est finalement plainte par écrit le 27 janvier 2020. Au terme d'une enquête interne, la Ville Z a confirmé que le Registre National avait été illicitement consulté par un.e de ses employé.es.

4. La Ville Z a confirmé la consultation illicite des données personnelles de la plaignante reprises au Registre National. L'administration de la Ville Z écrit notamment ce qui suit, dans un courrier à la plaignante daté du 24 février 2020 :

5. « *Au regard des résultats obtenus, nous constatons en effet une consultation sur base de votre identité réalisée le 30 mars 2017 depuis les guichets du service Population – Etat Civil situés à la Maison des citoyens. Les vérifications complémentaires effectuées aussi auprès de l'agent concerné ne nous ont malheureusement pas permis d'identifier le motif professionnel qui doit strictement être de vigueur lors de l'utilisation de l'accès aux données du Registre national.*

6. *Il est un fait certain que l'utilisation des données contenues au Registre national doit systématiquement faire l'objet d'une justification à des fins strictement professionnelles pour chaque consultation, conformément aux prérogatives spécifiques qui ont justifié l'obtention dudit accès par le service concerné. Les employés disposant de l'accès au Registre national sont informés notamment par le biais d'une charte de l'utilisateur qui reprend précisément les règles à observer scrupuleusement en matière de confidentialité et d'utilisation exclusivement professionnelle.*

7. *Partant du constat qu'il y a, dans ce cas précis, aucune conformité de la consultation, et ce d'autant que vous n'habitez pas sur le territoire Z et que vous n'aviez ni sollicité ni été sollicitée par le service concerné pour un quelconque motif, je tiens à vous informer que les dispositions nécessaires ainsi que les mesures adéquates ont été prises et actées auprès de notre Département des Ressources Humaines (…)* ».

8. Le Service d'Inspection constate dans son rapport du 27 octobre 2020 qu'aucun élément dans la plainte ne laisse apparaître qu'il y ait eu en l'espèce un traitement au sens de l'article 4.2) du RGPD des données de la plaignante issues du Registre national après le 25 mai 2018.

II. Motivation

9. En application de l'article 4 § 1er LCA, l'Autorité de protection des données (APD) est responsable du contrôle des principes de protection des données contenus dans le RGPD et d'autres lois contenant des dispositions relatives à la protection du traitement des données à caractère personnel dont la Loi du 8 août 1983 organisant un Registre national des personnes physiques.

10. En application de l'article 33 § 1er LCA, la Chambre Contentieuse est l'organe de contentieux administratif de l'APD. Elle est saisie des plaintes que le Service de Première Ligne (SPL) lui transmet en application de l'article 62 § 1er LCA, soit des plaintes recevables. Conformément à l'article 60 alinéa 2 LCA, les plaintes sont recevables si elles sont rédigées dans l'une des langues nationales, contiennent un exposé des faits et les indications nécessaires pour identifier le traitement de données à caractère personnel sur lequel elles portent et qui relèvent de la compétence de l'APD.

II.1- Quant à la qualité de responsable du traitement

11. La Chambre Contentieuse note que la plainte est dirigée contre la Ville Z, ainsi que contre Mme Y, employée administrative au service population de la Ville Z.

12. Conformément à l'article 4.7 du RGPD, il y a lieu de considérer comme le responsable du traitement: « la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement. »

13. Conformément aux Lignes directrices 07/2020 de l'EDPB[1], la Chambre Contentieuse évalue concrètement le rôle et la qualité du (des) responsable(s) du traitement concerné(s).

14. En l'occurrence, la Chambre Contentieuse constate que c'est bien la défenderesse (Ville Z) qui détermine les finalités et les moyens du traitement. En effet, les consultations du Registre National sont effectuées uniquement dans le cadre des missions de la Ville Z. C'est par ailleurs celle-ci qui met à disposition les moyens pour effectuer ce traitement (via ses systèmes informatiques). Elle doit donc être considérée comme un responsable de traitement.

15. La Chambre Contentieuse relève en outre que la plaignante ne dépose pas de preuve du fait que l'employé.e auteur de la consultation abusive est bien Mme Y. Bien que dans l'échange de courriers entre la plaignante et le responsable de la Ville Z, celui-ci reconnait qu'un.e employé.e du service a opéré la consultation litigieuse, l'identité précise de son auteur n'est pas mentionnée.

16. A toutes fins utiles, dans l'hypothèse où il serait prouvé que Mme Y est l'auteur de la consultation abusive, il conviendrait de souligner d'emblée que, comme le rappelle la CJUE dans son arrêt Wirtschaftsakademie du 5 juin 2018, « la notion de « responsable du traitement » vise l'organisme qui, « seul ou conjointement avec d'autres » détermine les finalités et les moyens du traitement de données à caractère personnel, cette notion ne renvoie pas nécessairement à un organisme unique et peut concerner plusieurs acteurs (…)». Que la défenderesse soit responsable de traitement pour les consultations de ses employés au Registre National ne signifie donc pas, dans le cas d'espèce, qu'elle seule corresponde à cette qualité. Il convient en effet de distinguer les consultations au Registre National dans le cadre des finalités de la défenderesse (la Ville Z), des consultations abusives opérées à des fins privées par Mme Y, employée de la Ville Z. Comme il est indiqué ci-dessous, bien qu'elle ait utilisé les moyens mis à sa disposition par la défenderesse, dans la mesure où Mme Y a opéré les consultations litigieuses en dehors du cadre de ses tâches en tant qu'employée de la défenderesse, Mme Y doit être considérée comme responsable de traitement pour ces consultations abusives spécifiquement.

17. Comme l'indique l'EDPB, ceci n'exempte néanmoins en rien la défenderesse, en tant que responsable du traitement, des consultations au Registre National, de son obligation d'assurer la sécurité des traitements. Cet aspect est développé infra (voir infra « II.3- Rappel de l'obligation de sécurité dans le chef du responsable de traitement »).

[1] EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 02 September 2020, point 12.

II.2- Quant à la consultation abusive

18. Suite à l'identification des responsables de traitement, la Chambre Contentieuse se penche à présent sur le traitement opéré.

19. La Chambre Contentieuse note que la consultation dénoncée par la plaignante date du 30 mars 2017. Elle a donc eu lieu à une date antérieure à l'entrée en application du RGPD. La Chambre Contentieuse n'est donc pas autorisée à en connaître.

20. En effet, la Chambre Contentieuse trouve le fondement légal de sa compétence dans la Loi du 3 décembre 2017 portant création de l'Autorité de protection des données (LCA) dont l'entrée en vigueur a été fixée, sauf exceptions, à la date du 25 mai 2018 (article 110 de la LCA). Si la Chambre Contentieuse est compétente au regard de traitements de données qui, certes, ont débuté avant le 25 mai 2018 mais perdurent aujourd'hui, elle ne l'est pas pour des traitements ponctuels qui seraient intervenus avant le 25 mai 2018[2], aucune rétroactivité n'ayant été prévue pour l'exercice dans le temps de sa compétence.

21. En l'occurrence, l'enquête menée par le Service d'Inspection consécutivement au dépôt de cette plainte n' a pas révélé des manquements postérieurs à la date du 25 mai 2018.

22. Sur la base des éléments du dossier dont elle a connaissance et des compétences qui lui ont été attribuées par le législateur en vertu de l'article 95, § 1er de la LCA, la Chambre Contentieuse statue sur la suite à réserver au dossier; en l'occurrence, la Chambre Contentieuse procède au classement sans suite de la plainte, conformément à l'article 95, § 1er, 3° de la LCA.

23. En cas de classement sans suite, la Chambre Contentieuse doit procéder à un examen et à une motivation par étapes de la manière précisée ci-dessous :

    -l'absence de perspective suffisante pour une condamnation entraîne un classement sans suite pour motif technique ;
    -une condamnation couronnée de succès est techniquement réalisable mais n'est pas souhaitable en raison de fondements relevant de l'intérêt général, entraînant un classement sans suite pour motif d'opportunité[3].

[2] Voir notamment décision de la Chambre Contentieuse nr. 64/2020 du 29 septembre 2020, § 62.

[3] Voir l'arrêt de la Cour d'appel de Bruxelles (Cour des marchés), 2 septembre 2020, n° 2020/5460, 18.

24. En cas de classement sans suite sur la base de plusieurs motifs, les motifs de classement sans suite (respectivement un classement sans suite pour motif technique et un classement sans suite pour motif d'opportunité) doivent être traités par ordre d'importance[4],[5].

25. Dans le cas présent, la Chambre Contentieuse procède à un classement sans suite pour motif technique. Le traitement dénoncé par la plaignante date du 30 mars 2017, et est donc antérieur à l'entrée en application du RGPD. La Chambre Contentieuse n'est donc pas autorisée à en connaître.

II.3- Rappel de l'obligation de sécurité dans le chef du responsable de traitement

26. Bien que le traitement en cause se situe en dehors de la compétence *ratione temporis* de la Chambre Contentieuse, celle-ci rappelle néanmoins à titre pédagogique, qu'en sa qualité de responsable de traitement, la défenderesse (la Ville Z) est tenue de mettre en œuvre les principes de protection des données et doit être en mesure de démontrer que ceux-ci sont respectés (principe de responsabilité – article 5.2. du RGPD).

27. Elle doit par ailleurs, toujours en sa qualité de responsable de traitement, mettre en œuvre toutes les mesures nécessaires à cet effet (article 24 du RGPD). La Chambre Contentieuse insiste, comme elle a déjà eu l'occasion de le rappeler dans de précédentes décisions prises à l'encontre de mandataires publics[6], sur le fait que le secteur public, doit, de manière générale, être vecteur d'exemple dans les mesures qu'il adopte pour garantir le respect du droit fondamental à la protection des données personnelles.

II.3.1- Les contours de l'obligation de sécurité

28. Sur base de l'article 5.1.f RGPD, les données à caractère personnel doivent être traitées de façon à garantir une sécurité appropriée, « y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées».

---

[4] *Ibidem.*

[5] Cf Politique de classement sans suite de la Chambre Contentieuse, 18/06/2021, point 3 (« Dans quels cas ma plainte est-elle susceptible d'être classée sans suite par la Chambre Contentieuse? »), disponible sur https://www.autoriteprotectiondonnees.be/publications/politique-de-classement-sans-suite-de-la-chambre-contentieuse.pdf

[6] Voy décisions 10/2019 et 11/2019 de la Chambre Contentieuse du 25 novembre 2019 aux termes desquelles la Chambre Contentieuse rappelle que la qualité de mandataire public des responsables de traitement mis en cause aurait dû s'accompagner d'un comportement exemplaire au regard du respect de la législation, en ce compris celle relative à la protection des données personnelles.

29. En l'absence de mesures appropriées pour sécuriser les données à caractère personnel des personnes concernées, l'effectivité des droits fondamentaux à la vie privée et à la protection des données à caractère personnel ne peut être garantie, à fortiori au vu du rôle crucial joué par les technologies de l'information et de la communication dans notre société.

30. Il convient de relever que les principes d' « intégrité, confidentialité et disponibilité » repris à l'article 5,1,f) sont désormais érigés dans le RGPD au même rang que les principes fondamentaux de licéité, transparence, loyauté.

31. Les obligations des responsables de traitement quant à la sécurité des traitements reposent dans les articles 32 et suivants du RGPD.

32. Les composantes classiques des recommandations en termes de sécurité de l'information, telles que préconisées par la suite ISO27xxx sont la confidentialité des données, leur intégrité et leur disponibilité. A celles-ci s'ajoute la notion d'imputabilité, « qui permet de pouvoir identifier, pour toutes les actions accomplies, les personnes, les systèmes ou les processus qui les ont initiées (identification) et de garder trace de l'auteur et de l'action (traçabilité) ». L'imputabilité s'exprime notamment de façon concrète par la tenue d'un registre des log files selon le principe de journalisation des accès.

33. La journalisation consiste donc à l'enregistrement des informations pertinentes concernant les évènements d'un système informatique (accès au système ou à un de ses dossiers, modification d'un fichier, transfert de données…) dans des fichiers appelés « log files ». Les informations reprises sont entre autres les données consultées, la date, le type d'évènement, les données permettant d'identifier l'auteur de l'évènement, ainsi que le motif de cet accès. Ceci permet notamment d'identifier toute consultation des données personnelles abusive ou pour une finalité non légitime, ou encore de déterminer l'origine d'un accident.

34. Bien que la journalisation ne soit pas expressément mentionnée dans le RGPD, la tenue d'un journal des log files constitue une mesure technique et organisationnelle envisagée dans l'article 32 RGPD. Elle constitue une bonne pratique, recommandée à tout responsable de traitement. Ces mesures doivent être adaptées aux risques.

35. L'institution prédécesseur de l'APD (la Commission de la Vie Privée –CPVP ci-dessous-) indiquait déjà dans ses Lignes directrices pour la sécurité de l'information de données à

caractère personnel ainsi que dans ses Recommandations aux villes et communes concernant les registres de logs IT que la journalisation constitue un élément incontournable de toute politique de sécurité de l'information, en ce qu'elle permet la traçabilité des accès aux systèmes informatiques.

II.3.2-Lien entre les obligations de sécurité des responsables de traitement et les principes de responsabilité et transparence

36. Comme indiqué supra, l'article 32 RGPD doit être lu en combinaison avec l'article 5.2 RGPD et l'article 24 RGPD, soumettant le responsable du traitement au principe de responsabilité. Il incombe au responsable du traitement de démontrer son respect des dispositions du RGPD, en prenant des mesures techniques et organisationnelles appropriées, de façon transparente et traçable, permettant en cas de contrôle d'apporter la preuve des garanties appliquées.

37. Le principe de responsabilité, lu en conjonction avec le principe de transparence (article 5.1.a RGPD), permet aux personnes concernées d'exercer leurs droits et de contrôler la conformité des traitements opérés sur leurs données à caractère personnel. Elle permet ainsi d'assumer la responsabilité .

38. Le considérant 63 du RGPD ajoute en outre à cela que ce droit d'accès doit être considéré comme un mécanisme de contrôle : "*Une personne concernée devrait avoir le droit d'accéder aux données à caractère personnel qui ont été collectées à son sujet et d'exercer ce droit facilement et à des intervalles raisonnables, afin de prendre connaissance du traitement et d'en vérifier la licéité*."

39. Ces principes de responsabilité et de transparence s'articulent avec l'article 15 du RGPD, qui garantit le droit d'accès de la personne concernées à ses données personnelles traitées. La CPVP concluait déjà à l'égard de la journalisation, de façon univoque:

40. « *Un fichier de journalisation incomplet et une absence de mention du motif de la consultation constituent une atteinte à l'exercice utile du droit d'accès et de contrôle dont dispose la personne concernée. Cela compromet également l'exercice des autres droits tels que le droit de rectification (article 16 du RGPD), le droit à l'oubli (article 17 du RGPD), et le droit à la limitation de l'utilisation de données traitées de façon illicite (article 18 du RGPD)*. » (p10)

41. La Chambre Contentieuse recommande la tenue d'un registre journal des log files en tant que bonne pratique, dans la mesure où la journalisation est utile pour tout responsable de traitement, en ce qu'elle permet d'assurer la matérialisation du principe de disponibilité, lui-même étroitement lié aux principes de confidentialité et d'intégrité des données.

42. Par ailleurs, parmi les mesures de sécurité adaptées destinées à garantir la confidentialités des données, un responsable de traitement tel que la défenderesse est nécessairement tenu de mettre en place des mesures de sécurité organisationnelles et techniques qui garantissent un contrôle des accès[7] : en d'autres termes, seules les personnes qui, dans l'exercice de leur fonction propre, ont besoin d'accéder à telle ou telle donnée doivent pouvoir bénéficier des accès nécessaires à cet effet.

43. La Chambre Contentieuse rappelle à cet égard l'article 5.1.b) RGPD qui consacre le principe de finalité, soit l'exigence que les données soient collectées pour des finalités déterminées, explicites et légitimes et ne soient pas traitées ultérieurement d'une manière incompatible avec ces finalités. A cet égard, la défenderesse est autorisée à consulter le Registre national pour des finalités déterminées conformément à la Loi du 8 août 1983 organisant un Registre national des personnes physiques.

44. Le responsable de traitement doit donc s'assurer que les données à caractère personnel ne sont accessibles qu'aux personnes et aux applications qui en ont explicitement l'autorisation. Il convient d'attribuer à chaque personne son propre compte et l'accès aux données à caractère personnel devrait être exclusivement autorisé en appliquant les principes du besoin d'en connaître. Ces personnes devraient uniquement avoir accès à la

---

[7] Voy. notamment les Mesures de référence en matière de sécurité applicables à tout traitement de données à caractère à personnel édictées par la Commission de la protection de la vie privée : https://www.autoriteprotectiondonnees.be/lexique/mesures-de-reference

« Sécurisation logique des accès

L'organisme doit s'assurer que les données à caractère personnel ne soient accessibles, conformément à leur classification, qu'aux personnes et aux applications qui en ont explicitement l'autorisation.

Il maintiendra à jour une liste actualisée des différentes personnes habilitées à accéder et traiter ces données et de leurs pouvoirs respectifs (création, consultation, modification, destruction).

Ces différentes autorisations doivent être traduites en dispositifs techniques et contrôles d'accès aux différents éléments informatiques (programmes, procédures, éléments de stockage, équipements de télécommunication, etc.) intervenant dans le

traitement des données à caractère personnel.

Ces dispositions techniques doivent inclure les activités en amont (développement applicatif) et en aval (gestion des exemplaires

de sauvegarde).

Si le niveau de sécurité l'impose, l'identification des intervenants sera complétée par une procédure d'authentification. »

fonctionnalité ou aux données dont elles ont besoin aux fins de l'exécution des tâches qui leur sont dévolues et ce, dans le respect du principe de finalité.

45. Il incombe donc à la défenderesse de garantir que l'accès au Registre national demeure limité aux finalités pour lesquelles cet accès a été autorisé. Il lui incombe également d'être en mesure de le démontrer. Le respect du principe de finalité, pilier de la protection des données, ne peut en effet pas être vérifié si les agents d'une structure telle la défenderesse n'enregistrent pas le motif de la consultation qu'ils opèrent. Il est tout aussi essentiel à cet égard que conformément à l'article 24 du RGPD, la défenderesse dispose d'un mécanisme de contrôle adéquat garantissant que ses agents habilités consultent le Registre national dans le cadre de ces seules finalités. La défenderesse doit disposer d'une application informatique qui permette de légitimer chaque consultation effectuée par son personnel et démontre ainsi que la consultation a eu lieu dans le cadre de l'exercice des tâches du membre du personnel qui a effectué la consultation.

46. 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.

47. Conformément à sa politique de classement sans suite, la Chambre Contentieuse communiquera la décision pour information aux parties défenderesses[8].

[8]https://www.autoriteprotectiondonnees.be/publications/politique-de-classement-sans-suite-de-la-chambre-contentieuse.pdf (titre 5 Le classement sans suite sera-t-il publié ? la partie adverse en sera-t-elle informée ?)

PAR CES MOTIFS,

en vertu de l'article 95, § 1er, 3° de la loi du 3 décembre 2017 *portant création de l'Autorité de protection des données*, la Chambre Contentieuse de l'Autorité de protection des données décide de classer la présente plainte sans suite.

En vertu de l'article 108, § 1er de la loi du 3 décembre 2017, cette décision peut faire l'objet d'un recours dans un délai de trente jours, à compter de la notification, à la Cour des marchés.

(sé). Hielke Hijmans

Président de la Chambre Contentieuse