Autorité de protection des données
Gegevensbeschermingsautoriteit

Chambre Contentieuse

Décision quant au fond 129/2021 du 26 novembre 2021

Numéro de dossier : DOS-2019-03353

Objet : Plainte pour consultation du registre national par une employée communale

La Chambre Contentieuse de l'Autorité de protection des données (ci-après APD), constituée de Monsieur Hielke Hijmans, président et de Messieurs Yves Poullet et Frank De Smet;

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 plaignant : X, représenté par Maître Gérald Horne, ci-après “le plaignant” ;

La défenderesse : Commune Y, représentée par Maître Jean Proesmans, ci-après la "défenderesse”.

I. Faits et rétroactes

1. Le 13 mai 2019, le plaignant envoie un email auprès de la commune en demandant si tout était en ordre concernant sa participation aux élections communales, étant donné qu'il sera à l'étranger au moment des élections.

2. A une date indéterminée, le service électoral de la commune a reçu des services postaux, le retour de la convocation électoral adressée au plaignant, sur laquelle est apposée la mention « ne reçoit pas/plus le courrier à l'adresse indiquée ». En conséquence de ceci, la commune décide d'initier une enquête concernant une éventuelle radiation de domicile.

3. Le 22 mai 2019, le plaignant est contacté par voie téléphonique par une fonctionnaire de police dans le cadre de cette enquête. Le même jour, le plaignant contacte la commune en lui faisant part de son étonnement quant à cette démarche. La commune confirme, toujours le même jour, par retour de courriel qu'une enquête pour vérification d'adresse est bien en cours.

4. Il s'ensuite un échange d'emails entre le plaignant et la commune durant lequel celui-ci sollicite des explications plus détaillées sur les raisons de l'enquête.

5. Il ressort également de la plainte que le plaignant est un ancien Conseiller communal d'opposition en litige avec la Bourgmestre devant les tribunaux.

6. Le 2 juin 2019, le plaignant s'adresse à un fonctionnaire qu'il estime être le délégué à la protection des données de la commune en joignant les échanges avec l'employée communal et demandant un rendez-vous pour éclaircir la situation à l'amiable.

7. Le 12 juin 2019, le plaignant envoie un document intitulé « plainte RGPD » à la commune avec copie à la Bourgmestre. Ce document reprend les griefs déjà portés à l'encontre de la commune dans les échanges précédents et indique pour la première fois que la compagne du frère du plaignant aurait consulté le registre national du plaignant dans un contexte privé.

8. Le 13 juin 2019, le Directeur général adjoint de la commune répond au plaignant, indiquant que la personne à qui le document « Plainte RGPD » était adressé n'est pas le délégué à la protection des données. Il répond à différentes questions du plaignant, et indique avoir suggéré à l'employée communal concernée (par la consultation du registre national) « d'envisager un règlement intrafamilial ». Le plaignant répond à ce courriel le même jour en demandant plus d'informations quant à l'identité du délégué à la protection des données et quant à la consultation de ses données au registre national.

9. Le 15 juin 2019, le plaignant introduit sa plainte auprès de l'APD. Le Service de première ligne indique au plaignant que le formulaire doit être signé. Un formulaire de plainte signé est renvoyé par le plaignant le 15 aout 2019.

10. Celle-ci porte sur une consultation irrégulière du registre national du plaignant par un membre du service communal et sur une enquête pour radiation du plaignant de l'adresse à laquelle il réside. Le 3 octobre 2019, la plainte est déclarée recevable par le Service de première ligne sur la base des articles 58 et 60 LCA et transmise à la Chambre Contentieuse sur la base de l'article 62, §1er LCA.

11. Le 17 mars 2020, la Chambre Contentieuse décide de traiter le dossier sur le fond sur base des articles 95, §1, 1° et 98 LCA.

12. Le même jour les parties concernées sont informées par courrier recommandé des dispositions énoncées à l'article 95, §2, ainsi que de celles de l'article 98 LCA. Les parties sont également informées du calendrier d'échange de conclusions sur la base de l'article 99 LCA.

    Le même courrier indique que la plainte « concerne la consultation des données personnelles du plaignant dans les registres de la population par un(e) employé(e) de l'administration communale en violation des règles de protection des données applicables. » Les éléments concernant la question de la résidence du plaignant et l'envoi de la convocation électorale ne sont donc pas examinés par la Chambre contentieuse, dans la mesure où ils concernent des questions de droit administratif et de police communale.

    En ce qui concerne les conclusions sur l'objet de la plainte, le délai de réception de la réponse de la défenderesse est fixé au 15 avril 2020, celui de la réplique du plaignant au 30 avril 2020 et enfin celui de la réplique de la défenderesse au 15 mai 2020.

13. Le 9 avril 2020, la défenderesse accepte que toutes les communications concernant l'affaire se fassent par voie électronique.

14. Le 15 avril 2020, la partie défenderesse fait parvenir sa conclusion en réponse à la Chambre Contentieuse. Elle y développe de nombreux points, dont certaines ne sont pas liés au cadre de la décision sur le fond, tel que défini au point 12 et qui porte précisément sur la consultation des données du registre national du plaignant. Ce point précis est abordé à partir de la page 22 des conclusions de la défenderesse, qui y relate les éléments suivants :

    - Qu'une employée de la commune, non habilitée à consulter le registre national a fait appel à une autre employée, habilitée elle, afin de consulter les données personnelles du plaignant, et ce « pour un motif précis inconnu, concernant un litige familial ».

    - Qu'une réprimande aurait été infligée à l'employée en question et qu'une note de service a été adressée à l'ensemble du personnel concernant le respect de la législation applicable en matière de protection des données personnelles.

    - Un chantier de mise en conformité avec le RGPD était déjà en chantier dans la commune au moment de la plainte. Celui-ci consistait par exemple à sensibiliser les agents de la commune,

effectuer un inventaire des traitements, effectuer un état des lieux des risques identifiés… La concluante précise que l'employée communale non-habilitée avait suivi cette sensibilisation.

- Qu'un incident tel que celui décrit dans la plainte ne pourrait plus se reproduire et qu'elle sollicite donc un non-lieu ou éventuellement un classement sans suite de la plainte.

15. Le 29 avril 2020, le plaignant fait parvenir sa conclusion en réplique à la Chambre contentieuse. Il y fait également part de plusieurs éléments qui dépassent le cadre de cette décision sur le fond (voir point 12). Sur la question de l'accès au registre national il invoque les points suivants :

- Les agents sont en aveu et les faits sont établis ;
- Le service public est responsable de la faute de ses agents et la commune est donc responsable de de cette faute ;
- Avant dire droit, il demande de recourir au Service d'inspection pour instruire davantage le dossier quant aux listings de consultation et en interrogeant les deux employées.

16. Le 18 mai 2020, la défenderesse indique ne pas avoir de conclusions en réplique et demande à être entendue.

17. Le 28 septembre 2021 , les parties sont informées du fait que l'audition aura lieu le 16 novembre 2021.

18. Le 16 novembre 2021, les parties sont entendues par la Chambre contentieuse. Au cours de cette audition, les points suivants ont été clarifiés :

- Il est reconnu par les deux parties qu'une employée communale (la belle sœur du plaignant) a consulté le registre national du plaignant, avec l'aide d'une autre employée communale qui y avait accès, pour des motifs privés.
- La finalité précise de cette consultation reste inconnue. La défenderesse la relie à un motif d'ordre successoral, tandis que le plaignant considère qu'il n'y a pas lien entre ces deux situations.
- les deux employées concernées (et non une seule comme le relataient les conclusions de l'avocat) ont été réprimandées de manière orale par le directeur de l'administration communale, après consultation du DPO ;
- la liste des logins fournie par la défenderesse dans ses conclusions provient du système du RN lui-même. Il ne permet pas la traçabilité des finalités de la consultation ;
- Un nouveau système interne à la commune et en train d'être mis en place, qui devrait contenir un système de traçabilité des finalités. Ceci devrait être réalisé pour le 15 décembre 2021.

19. Le 18 novembre 2021, le procès-verbal de l'audition est soumis aux parties.

II. Motivation

II.1. Identification du responsable de traitement

20. 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 physique.

21. Conformément à l'article 4.7 du RGPD, il y a lieu de considérer comme 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 ».

22. En l'occurrence, la Chambre Contentieuse constate que c'est bien la défenderesse 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 commune, bien que la finalité des consultations spécifiques qui ont eu lieu en l'espèce ne fait pas partie de ces missions. 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.

23. Il convient également de souligner 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 des consultations abusives opérées à des fins privées par une employée communale. Comme il est indiqué ci-dessous, bien qu'elle ait utilisé les moyens mis à sa disposition par la défenderesse, dans la mesure où la belle-sœur du plaignant a opéré les consultations litigieuses en dehors du cadre de ses tâches en tant qu'employée de la défenderesse, elle doit être considérée comme responsable de traitement pour ces consultations abusives spécifiquement.

24. 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 ensuite. Par ailleurs, la belle-sœur du plaignant n'ayant été visée par la plainte déposée auprès de l'APD, elle n'est pas partie à la présente procédure. Pour cette raison, la Chambre contentieuse n'effectuera pas de constats additionnels à son égard.

II.2. Identification du traitement

25. L'accès à l'information contenue dans le registre national constitue un traitement de données à caractère personnel au sens de l'article 4.2 du RGPD. En vertu de cette qualification, ce traitement, est soumis aux différents prescrits et obligations du RGPD et notamment aux principes de licéité, de loyauté et de transparence prévus à l'article 5.1.a du RGPD.

26. Le principe de licéité indique que tout traitement de données à caractère personnel doit disposer d'une des bases de licéité listées à l'article 6.1 du RGPD.

27. Il ressort des conclusions de la défenderesse que celle-ci revendique la base de licéité de l'article 6.1.e) du RGPD pour les traitements de données issues du registre national. Cet article est rédigé comme suit :

« Article 6

Licéité du traitement

1. Le traitement n'est licite que si, et dans la mesure où, au moins une des conditions suivantes est remplie:

[…]

e) le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement; »

Selon la défenderesse, cette mission d'intérêt public lui est octroyée par les normes suivantes :

- La loi 8 du août 1983 organisant un Registre national des personnes physiques ;
- L'arrêté royal du 3 avril 1984 relatif à l'accès de certaines autorités publiques au Registre national des personnes physiques, ainsi qu'à la tenue à jour et au contrôle des informations ;
- Loi du 19 juillet 1991 relative aux registres de la population, aux cartes d'identité, aux cartes des étrangers et aux documents de séjour ;
- L'arrêté royal du 16 juillet 1992 relatif aux registres de la population et au registre des étrangers ;
- Les instructions générales concernant la tenue des registres de la population (circulaire du 07/10/1992 relative à la tenue des registres de la population et des étrangers).

28. Ces différentes lois imposent aux communes certaines obligations concernant la tenue et la mise à jour des informations du Registre national et des registres de la population. Elles y ont également accès pour l'exercice de leur missions et sont soumises à certaines conditions dans ce cadre. Le fait pour une personne de communiquer des informations obtenues du Registre national à des personnes non habilitées à les recevoir, ou de faire usage de ces données à des fins autres que celles pour lesquelles elle a été légalement habilitée est sanctionné pénalement[1].

29. Il apparait des pièces du dossier et des conclusions des parties que le registre national du plaignant a bien fait l'objet d'un accès non-autorisé, et que cet élément est reconnu par la défenderesse elle-même. Elle indique que l'accès non-autorisé à eu lieu le 27 mai 2019 du fait d'une consultation par une employée communale, aidée par une collègue, dans le cadre d'un litige successoral d'ordre privé.

30. En réponse à cet incident, la défenderesse aurait mis en place plusieurs actions afin d'éviter une répétition de ce genre d'actes. L'employée en question aurait été réprimandée et une note de service rappelant le respect de la législation applicable en matière de protection des données a été envoyée à l'ensemble de son personnel. La Chambre contentieuse estime donc que les faits rapportés par le plaignant au sujet de la consultation de son dossier de registre national sont avérés.

31. Etant établi dans le dossier et reconnu par la défenderesse que le traitement de données a été effectué à des fins privées par une employée de la défenderesse, il ne peut être considéré que celui-ci entre dans la mission d'intérêt public de la défenderesse. L'employée communale étant considérée comme responsable de traitement à part entière, la Chambre estime que le traitement qu'elle a effectué pourrait constituer une violation du principe de licéité établi à l'article 5.1.a du RGPD. Dès lors que cette employée ne fait pas partie de la présente procédure, la Chambre contentieuse n'examinera pas plus en détail son rôle et son respect des normes réglementant la protection des données.

32.

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

33. Par ailleurs, la Chambre Contentieuse rappelle, qu'en sa qualité de responsable de traitement, la défenderesse 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).

34. 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[2], sur le fait que le secteur public, doit, de manière générale, être vecteur d'exemple dans les

[1] Loi 8 du août 1983 organisant un Registre national des personnes physiques, article 13.

[2] 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

mesures qu'il adopte pour garantir le respect du droit fondamental à la protection des données personnelles.

35. 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».

36. 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, *a fortiori* au vu du rôle crucial joué par les technologies de l'information et de la communication dans notre société.

37. Il convient de relever que le principe de sécurité' repris à l'article 5.1.f est désormais érigé dans le RGPD au même rang que les principes fondamentaux de licéité, transparence, loyauté.

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

39. 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.

40. La journalisation consiste donc à enregistrer 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. 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 au responsable de traitement lorsque cette mesure est adaptée aux risques lié aux caractéristiques du traitement. .

41. 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[3].

42. Cette pratique a par ailleurs été consacrée par le législateur qui a intégré cette obligation dans l'article 17 de la loi du 8 aout 1983 organisant un registre national des personnes physiques. Cet article est reproduit ci-dessous :

Art. 17. Chaque autorité publique, organisme public ou privé ayant obtenu l'autorisation d'accéder aux informations du Registre national des personnes physiques, en ce compris les services de police, ainsi que ceux de la Justice cités aux articles 5 et 8 doit être en mesure de pouvoir justifier les consultations effectuées, que celles-ci se fassent par un utilisateur individuel ou par un système informatique automatique. A cet effet, afin d'assurer la traçabilité des consultations, chaque utilisateur tient un registre des consultations. Ce registre indique l'identification de l'utilisateur individuel ou du processus ou du système qui a accédé aux données, les données qui ont été consultées, la façon dont elles ont été consultées, à savoir en lecture ou pour modification, la date et l'heure de la consultation ainsi que ***la finalité pour laquelle les données du Registre national des personnes physiques ont été consultées****. Le registre des consultations est conservé au moins 10 ans à partir de la date de la consultation. Il est également certifié.*

Le registre des consultations est tenu à la disposition de l'Autorité de protection des données.

Les services du Registre national des personnes physiques tiennent également un registre des consultations des utilisateurs et communications effectuées.

Ce registre indique l'identification de l'utilisateur qui a accédé aux données ou obtenu communication de celles-ci, les données qui ont été consultées ou communiquées, la façon dont elles ont été consultées, à savoir en lecture ou pour modification, ou communiquées, la date et l'heure de la consultation ou de la communication.[4]

43. Il ressort des conclusions de la partie défenderesse et de l'audition qu'un tel système permettant l'enregistrement de la finalité du traitement n'existait pas au moment du traitement litigieux. Selon le Délégué à la protection des données, un nouveau système intégrant cette fonctionnalité serait en développement et devrait être opérationnel au 15 décembre 2021.

44. Au vu des éléments exposés ci-dessus, la Chambre contentieuse conclut donc qu'il y a eu violation de l'article 32 du RGPD puisque la partie défenderesse ne disposait pas au moment des faits et ne dispose toujours pas à l'heure actuelle des mesures techniques et organisationnelles nécessaires pour assurer la sécurité des données du registre national, dans le sens où elle ne dispose pas d'un système permettant la journalisation des finalités des consultations. Cette violation est d'autant plus

[3] CPVP, Recommandation n° 07/2017 du 30 août 2017.

[4] C'est la Chambre contentieuse qui souligne.

caractéristique que l'article 17 de la Loi organisant un registre national impose spécifiquement ces obligations, qui, en l'espèce, ne sont pas respectées par la partie défenderesse.

II.4. Lien entre les obligations de sécurité des responsables de traitement et les principes de responsabilité et transparence

45. 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. À titre pédagogique, la Chambre contentieuse rappelle qu'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. 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 .

46. Le considérant 63 du RGPD ajoute que le 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."

47. 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:

« 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). »[5]

48. 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. La Chambre contentieuse précise par ailleurs, qu'il s'agit d'une obligation légale inscrite dans la loi organisant le registre national, telle que modifiée par la par la Loi du 25 novembre 2018 portant des dispositions diverses concernant le Registre

[5] CPVP, Recommandation n° 07/2017 du 30 août 2017, p. 10.

national et les registres de population qui est entrée en vigueur le 24 décembre 2018, soit avant les faits litigieux.

49. Par ailleurs, parmi les mesures de sécurité adaptées destinées à garantir la confidentialité des données, un responsable de traitement tel que la défenderesse est selon le point de vue exprimé à l'époque par la Commission belge de protection de la vie privée tenu de mettre en place des mesures de sécurité organisationnelles et techniques qui garantissent un contrôle des accès[6]: 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.

50. La Chambre Contentieuse rappelle à cet égard l'article 5.1.b du 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.

51. 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 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.

52. 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 permet 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.

53. La Chambre contentieuse rappelle qu'elle a par le passé pris des décisions concernant le sujet de l'accès aux données du registre national. Ainsi, la décision 19/2020[7] impose notamment que le responsable de traitement ayant accès aux données du Registre national mette en place un contrôle

[6] 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

[7] Décision 19/2020 du 29 avril 2020 (disponible à https://www.autoriteprotectiondonnees.be/publications/decision-quant-au-fond-n-19-2020.pdf)

des accès, et garantisse 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. Ces obligations sont déduites par la Chambre contentieuse notamment des articles 5.1.b et f, 5.2., 24, 32 du RGPD et de l'article 17 de la Loi du 8 août 1983 organisant un Registre national des personnes physiques.

III. Quant aux mesures correctrices et aux sanctions

54. Aux termes de l'article 100 LCA, la Chambre Contentieuse a le pouvoir de:

1° classer la plainte sans suite;
2° ordonner le non-lieu;
3° prononcer une suspension du prononcé;
4° proposer une transaction;
5° formuler des avertissements ou des réprimandes;
6° ordonner de se conformer aux demandes de la personne concernée d'exercer ces 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 Etat 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.

55. La Chambre contentieuse souligne qu'en vertu de l'article 221.2° de la Loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, elle ne peut imposer d'amende à la défenderesse, puisque celle-ci est une autorité publique au sens de l'article 5.1° de cette même loi.

56. La Chambre contentieuse a constaté une violation de l'article 32 du RGPD (point 44).

57. En conclusion de ce qui précède, et au vu de toutes les circonstances de l'espèce, la Chambre Contentieuse estime que la réprimande (soit le rappel à l'ordre visé à l'article 58.2.b du RGPD) est en l'espèce, la sanction effective, proportionnée et dissuasive qui s'impose à l'égard de la défenderesse[8].

58. La Chambre contentieuse a pris bonne note du fait que la partie défenderesse a indiqué lors de l'audition que le déploiement de son nouveau système informatique devrait lui permettre de combler les lacunes identifiées par la Chambre contentieuse dans la présente décision. Afin de pouvoir confirmer l'effectivité de cette modification mise en œuvre par la partie défenderesse, la Chambre contentieuse lui ordonne de lui faire parvenir, dans les quatre mois qui suivent l'adoption de la présente décision, les pièces démontrant la mise en œuvre effective d'un système de journalisation des consultations permettant notamment l'enregistrement de la finalité du traitement.

IV. Publication de la décision

59. Compte tenu de l'importance de la transparence en ce qui concerne le processus décisionnel et au vu des précédents de la Chambre Contentieuse, cette décision sera publiée sur le site Internet de l'Autorité de protection des données moyennant la suppression des données d'identification directe des parties et des personnes citées, qu'elles soient physiques ou morales.

[8] Comme elle a déjà eu l'occasion de la préciser dans plusieurs décisions, la Chambre Contentieuse rappelle ici que l'avertissement sanctionne un manquement qui est susceptible de se produire: voy. l'article 58.2.a) du RPD à cet égard.

POUR CES MOTIFS,

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

- D'imposer une **réprimande pour violation de l'article 32 du RGPD**, sur base de l'article 100, 5° LCA.

- D'imposer une **mise en conformité du traitement dans un délai de quatre mois**, sur base de l'article 100, 6° LCA.

- D'ordonner à la défenderesse **d'informer, documents probants à l'appui, l'Autorité de protection des données** (Chambre Contentieuse) de la suite réservée à la présente décision et ce dans le même délai. Cette communication peut se faire par e-mail adressé à l'adresse suivante (adresse de contact de la Chambre Contentieuse): litigationchamber@apd-gba.be.

En vertu de l'article 108 §1er LCA, cette décision peut faire l'objet d'un recours auprès de la Cour des

(sé). Hielke Hijmans

Président de la Chambre Contentieuse