Autorité de protection des données
Gegevensbeschermingsautoriteit

Chambre Contentieuse

Décision 158/2023 du 30 novembre 2023

Numéro de dossier : DOS-2023-02046

Objet : Plainte relative à un problème de sécurité rencontré par une administration communale (piratage de la boîte mail de la directrice d'une école communale pour des tentatives de phishing) ; et à l'absence de réaction à une demande d'information et d'accès exercée par le plaignant

La Chambre Contentieuse de l'Autorité de protection des données, constituée de monsieur Romain ROBERT, désigné par le Président de la Chambre contentieuse en vertu de l'article 43 du Règlement d'Ordre Intérieur ;

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 : M. X, ci-après « le plaignant » ;

La défenderesse : L'administration communale Y, ci-après : « la défenderesse ».

I. Faits et procédure

1. Le 5 mai 2023, le plaignant a introduit une plainte auprès de l'Autorité de protection des données (ci-après « APD ») contre la partie défenderesse.
2. L'objet de la plainte concerne un incident de sécurité rencontré par l'administration communale Y (ci-après « la Commune ») ; et l'absence de réaction de ladite Commune à une demande d'information et d'accès exercée par le plaignant.
3. Le 17 juin 2022, le plaignant a reçu un courriel intitulé « alerte virus » signalant un incident de sécurité concernant le piratage de la boîte e-mail d'un employé de la Commune. Les faits suivants ont été mentionnés dans le courriel : - la boîte e-mail piratée appartient à Madame Z1, qui est la directrice de l'école communale fréquentée par l'enfant du plaignant ; - Il a été conseillé de ne pas consulter les e-mails provenant de cette boîte piratée mais de les supprimer ainsi que de ne pas cliquer sur le lien contenu dans le courriel (car il s'agit d'un lien de phishing). En outre, le courriel précise les actions à entreprendre selon la catégorie d'individus concernés (les employés ou ouvriers communaux, d'une part et les autres personnes, d'autre part).
4. En plus des faits susmentionnés, il ressort du formulaire de plainte et des annexes que :
   - des sources tierces anonymes auraient communiqué des informations supplémentaires sur l'incident, indiquant que le piratage aurait réussi. Selon les informations recueillies par le plaignant, la boîte e-mail piratée aurait été utilisée pour envoyer des courriers contenant des liens vers des fichiers malveillants qui auraient infecté d'autres systèmes informatiques. De plus, les e-mails auraient été manipulés et déplacés vers la corbeille, suggérant un accès potentiel à l'ensemble des informations contenues dans ces e-mails. ;
   - la boîte e-mail compromise pourrait potentiellement contenir de nombreuses informations sensibles protégées par le RGPD, telles que des échanges concernant des problèmes entre les enfants, des certificats médicaux et d'autres données personnelles. ;
   - le plaignant soulève des préoccupations quant à l'utilisation présumée des outils Office 365 par la commune, ce qui pourrait permettre « un accès aux documents en dehors du contexte d'Outlook de la directrice ». Toujours selon le plaignant, en cas d'accès non autorisé à ces documents, des informations supplémentaires à caractère personnel pourraient être compromises. La Commune n'a jamais confirmé ou informé l'utilisation des outils Office 365. Cependant, le plaignant signale qu'il aurait déjà partagé des fichiers avec la Commune, ce qui indique « l'usage de OneDrive et sa galaxie O365 ».

5. Le 3 avril 2023, le plaignant a contacté le Directeur Général de la commune, Monsieur Z2, pour obtenir des informations supplémentaires (exercice de son droit à l'information) et pour déterminer s'il était nécessaire d'agir en tant que parent. Les informations demandées dans le courriel sont les suivantes : confirmer la notification par la Commune auprès de l'APD conformément à l'article 33 du RGPD ; confirmer que les parents et les personnes concernées ont été informés de cette violation conformément à l'article 34 du RGPD ; fournir une copie des notifications précitées ; fournir des informations sur les mesures de sécurité mises en place pour prévenir de futures attaques et protéger les données à caractère personnel des citoyens ; fournir des informations sur les mesures d'audit et de contrôle mises en place pour assurer la sécurité des données dans l'ensemble de l'environnement cloud ; et fournir les documents contenant ses données personnelles qui sont stockées et traitées, ainsi que des informations sur les personnes qui y ont accès, conformément à son droit d'accès

6. Selon le plaignant, aucune réponse n'aurait été formulée à sa demande d'information, et il semblerait que personne d'autre n'ait été informé de l'incident.

   Le 9 mai 2023, le SPL déclare la plainte recevable sur la base des articles 58 et 60 de la LCA[1], et transmet celle-ci à la Chambre Contentieuse conformément à l'article 62, § 1 de la LCA[2].

II. Motivation

7. En application de l'article 4, § 1er de la LCA, l'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.

8. 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 de la LCA, soit des plaintes recevables. Conformément à l'article 60 alinéa 2 de la 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.

9. En application des articles 51 et s. du RGPD et de l'article 4, § 1er de la LCA, il revient à la Chambre Contentieuse en tant qu'organe de contentieux administratif de l'APD, d'exercer un contrôle effectif de l'application du RGPD et de protéger les libertés et droits

[1] En vertu de l'article 61 LCA, la Chambre Contentieuse informe les parties par la présente décision, du fait que la plainte a été déclarée recevable.
[2] En vertu de l'article 95, § 2 LCA, par la présente décision, la Chambre Contentieuse informe les parties du fait qu'à la suite de cette plainte, le dossier lui a été transmis.

fondamentaux des personnes physiques à l'égard du traitement et de faciliter le libre flux des données à caractère personnel au sein de l'Union.

10. L'article 15.1 du RGPD prévoient que la personne concernée peut s'adresser au responsable du traitement afin d'obtenir les informations, notamment au titre des articles 15 à 22 et 34 du RGPD.

11. En vertu de l'article 12.3 du RGPD, le responsable du traitement dispose d'un délai maximal d'un mois à compter de la demande de la personne concernée pour fournir une réponse. Ce délai peut, sous conditions, être prolongé de deux mois supplémentaires.

12. Il ressort des pièces du dossier que sur le site de la Commune, elle est la seule à être mentionnée comme responsable du traitement pour l'école concernée. Sans préjudice de l'attribution de cette qualité à d'autres entités, la présente décision est adressée à la Commune, présumée responsable du traitement dans le cas d'espèce.

13. En outre, même si la demande du plaignant ne vise pas spécifiquement les articles 15 à 22 du RGPD, il y a lieu de considérer *a priori* que la demande du plaignant était une demande d'accès aux informations entourant le traitement de ses données, au sens de l'article 15 du RGPD, en sus des informations au titre de l'article 34 du RGPD. La défenderesse ne semble pas avoir répondu à une telle demande, selon les informations dont la Chambre Contentieuse dispose.

14. De plus, la Chambre Contentieuse rappelle qu'en cas de violation des données à caractère personnel, le responsable du traitement est appelé à notifier l'APD et les personnes concernées dans les circonstances décrites par les articles 33 et 34 du RGPD. En l'absence d'éléments permettant d'établir une telle violation, la Chambre Contentieuse ne se prononce pas à cet égard, mais ceci sans préjudice de l'existence d'une violation des données et partant des articles 33 et 34 du RGPD, qui devrait être constatée suite à une plainte ou un rapport du Service d'Inspection de l'APD.

15. La Chambre Contentieuse estime que sur la base des faits susmentionnés, en ne répondant pas au plaignant, la défenderesse peut avoir commis une violation des articles 12 et 15 du RGPD.

16. Sur la base des faits décrits dans le dossier de plainte tels que résumés ci-dessus, et sur base des compétences qui lui ont été attribuées par le législateur en vertu de l'article 95, §1er de la LCA, la Chambre Contentieuse décide de procéder à la prise d'une décision conformément à l'article 95, § 1er, 5° de la LCA, plus précisément d'ordonner *au responsable du traitement de répondre au plaignant*.

17. 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 »[3] et pas une décision sur le fond de la Chambre Contentieuse au sens de l'article 100 de la LCA.

18. La présente décision a pour but d'informer la défenderesse, présumée responsable du traitement, du fait que celle-ci peut avoir commis une violation des dispositions du RGPD, afin de lui permettre d'encore se conformer aux dispositions précitées.

19. Si toutefois, le responsable du traitement 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 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. Le cas échéant, l'exécution de la présente décision sera suspendue pendant la période susmentionnée.

20. 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.

21. Dans une optique de transparence, la Chambre Contentieuse souligne enfin qu'un traitement de l'affaire sur le fond peut conduire à l'imposition des mesures mentionnées à l'article 100 de la LCA[4].

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

23. Si une des deux parties souhaite recourir à la possibilité de consulter et de copier le dossier (article 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] Section 3, Sous-section 2 de la LCA (articles 94 à 97 inclus).
[4] Art. 100. § 1er. La chambre contentieuse a le pouvoir de
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.

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.

PAR CES MOTIFS,

la Chambre Contentieuse de l'Autorité de protection des données décide, sous réserve de l'introduction d'une demande par la défenderesse d'un traitement sur le fond conformément aux articles 98 e.s. de la LCA :

- en vertu de l'article **58.2.c) du RGPD** et de l'article **95, § 1er, 5° de la LCA**, d'ordonner à la défenderesse de se conformer à la demande de la personne concernée d'exercer ses droits, plus précisément le droit à obtenir une réponse à sa demande sur la base des article 12 et 15 du RGPD, et ce dans le délai de 30 jours à dater de la notification de la présente décision ;
- d'ordonner à la défenderesse d'informer par e-mail l'Autorité de protection des données (Chambre Contentieuse) de la suite qui est donnée à cette décision, dans le même délai, via l'adresse e-mail litigationchamber@apd-gba.be ; et
- si la défenderesse ne se conforme pas en temps utile à ce qui lui est demandé ci-dessus, de traiter d'office l'affaire sur le fond, conformément aux **articles 98 e.s. de la LCA**.

Conformément à l'article 108, § 1 de la LCA, un recours contre cette décision peut être introduit, dans un délai de trente jours à compter de sa notification, auprès de la Cour des Marchés (cour d'appel de Bruxelles), avec l'Autorité de protection des données comme partie défenderesse.

Un tel recours peut être introduit au moyen d'une requête interlocutoire qui doit contenir les informations énumérées à l'article 1034*ter* du Code judiciaire[5]. La requête interlocutoire doit être

[5] La requête contient à peine de nullité :
1° l'indication des jour, mois et an ;
2° les nom, prénom, domicile du requérant, ainsi que, le cas échéant, ses qualités et son numéro de registre national ou numéro d'entreprise ;
3° les nom, prénom, domicile et, le cas échéant, la qualité de la personne à convoquer ;
4° l'objet et l'exposé sommaire des moyens de la demande ;
5° l'indication du juge qui est saisi de la demande ;
6° la signature du requérant ou de son avocat.

déposée au greffe de la Cour des Marchés conformément à l'article 1034*quinquies* du C. jud.[6], ou via le système d'information e-Deposit du Ministère de la Justice (article 32*ter* du C. jud.).

(sé). Romain ROBERT

Membre de la Chambre Contentieuse

[6] La requête, accompagnée de son annexe, est envoyée, en autant d'exemplaires qu'il y a de parties en cause, par lettre recommandée au greffier de la juridiction ou déposée au greffe.