Autorité de protection des données
Gegevensbeschermingsautoriteit

Chambre Contentieuse

Décision 33/2022 du 10 mars 2022

N° de dossier : DOS-2021-05171

Objet : Plainte relative à l'absence de réaction de la part du responsable du traitement à une demande d'accès et à l'insuffisance de mesures de sécurité, suite à un hacking informatique

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 RGPD;

Vu la Loi du 3 décembre 2017 *portant création de l'Autorité de protection des données (ci-après LCA)*;

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 LTD*) ;

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, ci-après « le plaignant », représenté par maître Geert Coene ;

Les défendeurs : Y1 et Y2 , ci-après « les défendeurs » ;

I. Faits et procédure

1. Le 8 juillet 2021, le plaignant a déposé plainte auprès de l'Autorité de protection des données (ci-après « APD ») contre les défendeurs, pour absence de réaction à une demande d'accès, ainsi que pour violation de l'obligation de sécurité, suite à un hacking informatique.

2. Le 7 décembre 2020, le plaignant a commandé un véhicule (..) d'une valeur de (.. EUR) et a payé un acompte de (..EUR) auprès des défendeurs.

3. Le 4 février 2021, une employée des défendeurs a envoyé un courriel au plaignant avec le numéro de compte bancaire sur lequel le solde restant dû devait être payé. Le 5 février 2021, le plaignant a reçu un nouveau courriel, envoyé depuis l'adresse mail de l'employée des défendeurs, qui stipulait que le compte bancaire initialement communiqué était « mauvais » et informait du nouveau numéro de compte sur lequel le transfert devait être effectué.

4. Le 8 février 2021, le plaignant a informé l'employée des défendeurs par courriel que le virement d'un montant de (..EUR) avait été ordonné. Le compte du plaignant a été débité le 9 février 2021. Le 11 février 2021, l'employée des défendeurs a indiqué dans un courriel que le montant restant dû n'avait pas été perçu et a demandé une preuve de paiement. Celle-ci a été annexée par le plaignant dans un courriel du 12 février 2021.

5. Le 15 mars 2021, le plaignant a appris qu'il avait été victime d'une escroquerie en ligne, l'adresse email de l'employée des défendeurs ayant probablement été usurpée. Selon le plaignant, l'employée en question et un cadre de la société auraient reconnu avoir été victimes d'un hacking informatique.

6. Le 17 mars 2021, le plaignant a porté plainte pour escroquerie avec Internet à la zone de police de Bruxelles Capitale Ixelles . À la même date, le directeur de la société a porté plainte pour escroquerie et piratage (hacking) sur Internet (« *hoofde van oplichting met internet en hacking* »)[1] à la zone de police de Zaventem .

7. Le 28 avril 2021, le plaignant a reçu un rapport d'un expert assermenté en informatique qu'il avait engagé à cet effet : le rapport indique que le serveur utilisé par la société a fait l'objet d'une « *brèche majeure [...] en ce début d'année 2021* », que cette brèche « *permettrait, entre autres, des usurpations d'identités* » mais que pour pouvoir conclure avec certitude à

[1] Zone de police de Zaventem, PV n°(..)

un hacking il faut des vérifications complémentaires pour lesquelles un mandat judiciaire est nécessaire.

8. Le 4 mai 2021, le plaignant a mis en demeure les défendeurs de communiquer l'intégralité des données personnelles à son égard dont ils disposent en précisant quelles données avaient fait l'objet du hacking. Selon le plaignant, les défendeurs n'ont pas donné suite à cette mise en demeure.

9. Le 17 juillet 2021, le Service de Première Ligne (SPL) de l'APD a déclaré la plainte recevable sur la base des articles 58 et 60 de la LCA et l'a transmise, en vertu de l'article 62, §1er de la LCA, à la Chambre Contentieuse.

II. Motivation

10. 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.

11. En application de l'article 33, §1er de la 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 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.

12. 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 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.

13. La Chambre Contentieuse note que le plaignant soulève **l'absence de réaction du responsable du traitement à la demande d'exercice de son droit d'accès conformément à l'article 15 du RGPD**.

14. La Chambre Contentieuse rappelle que le responsable du traitement doit donner suite à la demande formulée en application des articles 15 à 22 du RGPD par le plaignant, en l'espèce

une demande d'accès prévue par l'article 15 du RGPD (*exercice du droit d'accès*), et ce dans le respect des conditions fixées à l'article 12 du RGPD[2].

15. La Chambre Contentieuse souligne également qu'il incombe au responsable du traitement de fournir au plaignant des informations sur les mesures prises à la suite d'une demande formulée en application des articles 15 à 22 du RGPD, dans les meilleurs délais et en tout état de cause dans un délai d'un mois à compter de la réception de la demande. L'article 12.3 du RGPD prévoit que ce délai peut, au besoin, être prolongé de deux mois, compte tenu de la complexité et du nombre de demandes[3]. Dans un tel cas, le responsable du traitement informe le plaignant de cette prolongation et des motifs du report dans un délai d'un mois à compter de la réception de la demande [4].

16. Dans l'hypothèse où le responsable du traitement ne donne pas suite à la demande formulée par le plaignant, il informe celui-ci sans tarder et au plus tard dans un délai d'un mois à compter de la réception de la demande des motifs de son inaction et de la possibilité d'introduire une réclamation auprès d'une autorité de contrôle et de former un recours juridictionnel[5].

17. Sur la base des pièces étayant la plainte, la Chambre Contentieuse constate que le plaignant a exercé son droit d'accès conformément à l'article 15 du RGPD, mais que le responsable du traitement n'a donné aucune suite à la demande du plaignant.

18. La Chambre Contentieuse estime que le responsable du traitement n'a pas, *prima facie*, respecté les articles 12.3 et 12.4 du RGPD, ainsi que l'article 15.1 du RGPD, ce qui justifie en l'espèce de procéder à la prise d'une décision sur la base de l'article 95, § 1er, 5° de la LCA.

---

[2] Article 12.2 du RGPD. ; En vertu de l'article 15 du RGPD, « *1. La personne concernée a le droit d'obtenir du responsable du traitement la confirmation que des données à caractère personnel la concernant sont ou ne sont pas traitées et, lorsqu'elles le sont, l'accès auxdites données à caractère personnel ainsi que les informations suivantes: a) les finalités du traitement; b) les catégories de données à caractère personnel concernées; c) les destinataires ou catégories de destinataires auxquels les données à caractère personnel ont été ou seront communiquées, en particulier les destinataires qui sont établis dans des pays tiers ou les organisations internationales; d) lorsque cela est possible, la durée de conservation des données à caractère personnel envisagée ou, lorsque ce n'est pas possible, les critères utilisés pour déterminer cette durée; e) l'existence du droit de demander au responsable du traitement la rectification ou l'effacement de données à caractère personnel, ou une limitation du traitement des données à caractère personnel relatives à la personne concernée, ou du droit de s'opposer à ce traitement; f) le droit d'introduire une réclamation auprès d'une autorité de contrôle; g) lorsque les données à caractère personnel ne sont pas collectées auprès de la personne concernée, toute information disponible quant à leur source; h) l'existence d'une prise de décision automatisée, y compris un profilage, visée à l'article 22, paragraphes 1 et 4, et, au moins en pareils cas, des informations utiles concernant la logique sous-jacente, ainsi que l'importance et les conséquences prévues de ce traitement pour la personne concernée.* […] ».

[3] Article 12.3 du RGPD.

[4] Article 12.3 du RGPD.

[5] Article 12.4 du RGPD.

19. La Chambre contentieuse ordonne au responsable du traitement de se conformer à la demande d'exercice du droit d'accès du plaignant, et partant de lui fournir une copie de toutes les données à caractère personnel qu'il détient en précisant quelles données ont fait l'objet du hacking.

20. **Dans un deuxième temps**, la Chambre Contentieuse relève l'insuffisance des mesures de sécurité dans le chef des défendeurs, pointée par le plaignant.

21. La Chambre Contentieuse rappelle que **le responsable du traitement est soumis au principe de sécurité et de confidentialité consacré par les articles 5.1.f et 32 du RGDP**.

22. **En vertu des articles 5.1.f) et 32 du RGPD**, le responsable du traitement doit assurer la sécurité, l'intégrité et la confidentialité des données à caractère personnel qu'il détient à l'aide de mesures techniques et organisationnelles appropriées, notamment contre un traitement non-autorisé ou illégal et contre la perte, destruction ou altération accidentelle des données.

23. **Le considérant 83 du RGPD** envisage que « [...] le responsable du traitement [...] évalue les risques inhérents au traitement et [met] en œuvre des mesures pour les atténuer [...]. Ces mesures devraient assurer un niveau de sécurité approprié, y compris la confidentialité, compte tenu de l'état des connaissances et des coûts de mise en œuvre par rapport aux risques et à la nature des données à caractère personnel à protéger. Dans le cadre de l'évaluation des risques pour la sécurité des données, il convient de prendre en compte les risques que présente le **traitement de données à caractère personnel**, tels que la destruction, la perte ou 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, de manière accidentelle ou illicite, qui sont **susceptibles d'entraîner des dommages physiques, matériels ou un préjudice moral**. ».

24. **Le considérant 85 du RGPD** ajoute qu'« une violation de données à caractère personnel risque, si l'on n'intervient pas à temps et de manière appropriée, de causer aux personnes physiques concernées des dommages physiques, matériels ou un préjudice moral tels qu'une perte de contrôle sur leurs données à caractère personnel ou la limitation de leurs droits, une discrimination, un vol ou une usurpation d'identité, **une perte financière**, un renversement non autorisé de la procédure de pseudonymisation, une atteinte à la réputation, une perte de confidentialité de données à caractère personnel. ». Ainsi, **le considérant 87 du RGPD** invite le responsable du traitement à vérifier « si toutes les mesures de protection techniques et organisationnelles appropriées ont été mises en

œuvre pour établir immédiatement si une violation des données à caractère personnel s'est produite et pour informer rapidement l'autorité de contrôle et la personne concernée. »

25. **Le considérant 39 du RGPD** renforce l'idée que « les personnes concernées devraient être informées des risques, règles, garanties et droits liés au traitement des données à caractère personnel et des modalités d'exercice de leurs droits en ce qui concerne ce traitement [...]. ». À cet effet, **le considérant 86 du RGPD** prévoit que « le responsable du traitement [communique] une violation de données à caractère personnel à la personne concernée dans les meilleurs délais lorsque cette violation est susceptible d'engendrer un risque élevé pour les droits et libertés de la personne physique afin qu'elle puisse prendre les précautions qui s'imposent. La communication devrait décrire la nature de la violation des données à caractère personnel et formuler des recommandations à la personne physique concernée pour atténuer les effets négatifs potentiels. »

26. **Le considérant 88 du RGPD** déclare que « lors de la fixation de règles détaillées concernant la forme et les procédures applicables à la notification des violations de données à caractère personnel, il convient de tenir dûment compte des circonstances de cette violation, y compris du fait que **les données à caractère personnel étaient ou non protégées par des mesures de protection techniques appropriées, limitant efficacement la probabilité d'usurpation d'identité ou d'autres formes d'abus**. ».

27. Ensuite, la Chambre Contentieuse rappelle que **l'article 32 RGPD doit être lu en combinaison avec les articles 5.2, 24 et 25 du RGPD, soumettant le responsable du traitement au principe de responsabilité**.

28. **Selon l'article 24.1 du RGPD**, il incombe au responsable du traitement de mettre en œuvre « des mesures techniques et organisationnelles appropriés pour s'assurer et être en mesure de démontrer que le traitement est effectué conformément au [RGPD]. Ces mesures sont réexaminées et actualisées si nécessaire. ». Ensuite, l'article 24.2 du RGPD stipule que « lorsque cela est proportionné au regard des activités de traitement, les mesures [évoquées à l'article 24.1. du RGPD] comprennent la mise en œuvre de politiques appropriées en matière de protection des données par le responsable de traitement ».

29. **Le considérant 74 du RGPD** ajoute qu' « il importe, en particulier, que le responsable du traitement soit tenu de mettre en œuvre des mesures appropriées et effectives et soit à même de démontrer la conformité des activités de traitement avec le [RGPD], y compris l'efficacité des mesures. Ces mesures devraient tenir compte de la nature, de la portée, du

contexte et des finalités du traitement ainsi que du risque que celui-ci présente pour les droits et libertés des personnes physiques ».

30. Il incombe également au responsable du traitement, **en application de l'article 25 du RGPD**, d'intégrer le nécessaire respect des règles du RGPD en amont de ses actes et procédures (par exemple prévoir des mesures qui protègent l'adresse électronique des employés afin d'éviter le hacking informatique ; envisager des méthodes qui renforcent la sécurité des paiements ou encore la communication des coordonnées bancaires ; etc.).

31. En définitive, le responsable du traitement est tenu, sur base de l'article 32 du RGPD, d'assurer la sécurité des traitements, « compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques ». 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.

32. Sur la base des éléments de fait présents dans le dossier, la Chambre Contentieuse constate que :
    a. le responsable du traitement a organisé la communication des coordonnées bancaires par l'envoie d'un courrier électronique afin que le plaignant puisse finaliser son achat ;
    b. le plaignant a été victime d'une escroquerie en ligne, l'adresse email de l'employée du responsable du traitement ayant probablement été usurpée ;
    c. le rapport d'un expert assermenté en informatique indique que le serveur utilisé par le responsable du traitement a fait l'objet d'une « *brèche majeure [...] en ce début d'année 2021 », que cette brèche « permettrait, entre autres, des usurpation d'identités* » bien que pour pouvoir conclure avec certitude à un hacking des vérifications complémentaires sont requises pour lesquelles un mandat judiciaire est nécessaire ;
    d. la plainte déposée par le responsable du traitement pour escroquerie et piratage sur Internet amène à penser que le responsable du traitement reconnaît implicitement avoir été victime d'un hacking informatique ;
    e. l'usurpation de l'adresse email de l'employée du responsable du traitement a causé au plaignant un dommage matériel qui s'est traduit par une perte financière d'une valeur de (.. EUR).

33. La Chambre Contentieuse relève un manquement au respect des principes de sécurité et de responsabilité dans le chef du responsable du traitement. En effet, la Chambre Contentieuse souligne l'absence des mesures techniques et organisationnelles suffisantes envisagées par le responsable du traitement pour encadrer la communication sécurisée des coordonnées bancaires et ainsi garantir un paiement sécurisé. Pour rappel, le responsable du traitement vend des voiture de sport et de luxe, ce qui implique des transactions financières d'une valeur relativement élevée; qu'il convient que des mesures appropriées et effectives soient mise en œuvre par le responsable du traitement pour assurer la sécurité des traitements. De plus, le responsable du traitement doit également pouvoir démontrer la conformité des activités de traitements.
34. La Chambre Contentieuse note par ailleurs qu'aucune notification de fuite de données n'a été effectuée par les défenderesses auprès de l'APD, en violation de l'article 33 du RGPD.

35. Au regard de l'examen susmentionné, la Chambre Contentieuse estime que le responsable du traitement n'a pas, *prima facie*, respecté les articles 5.1.f et 5.2 du RGPD, ainsi que les articles 24 et 32 du RGPD, ce qui justifie en l'espèce de procéder à la prise d'une décision sur la base de l'article 95, § 1er, 4° de la LCA.

La Chambre contentieuse avertit la défenderesse au sens de l'article 58.2.a) du RGPD, qu'en l'absence de mise en conformité de son système informatique à son obligation d'assurer la sécurité des traitements , celle-ci se placerait en porte à faux vis-à-vis de son obligation de sécurité au sens du RGPD.

36. 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* », à différencier d'une décision sur le fond de la Chambre Contentieuse au sens de l'article 100 de la LCA.

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

38. 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 14 jours après la notification de la

présente décision. Le cas échéant, l'exécution de la présente décision est suspendue pendant la période susmentionnée.

39. 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.

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[6].

40. 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 par courrier ordinaire[7].

III. Publication de la décision

41. Vu l'importance de la transparence en ce qui concerne le processus décisionnel et les décisions de la Chambre Contentieuse, cette décision sera publiée sur le site Internet de l'Autorité de Protection des Données[8]. Il n'est toutefois pas nécessaire à cette fin que les données d'identification des parties soient directement communiquées.

---

[6] Article 100 de LCA stipule que « *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 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.* »

[7] Compte tenu des circonstances exceptionnelles actuelles et des mesures organisationnelles prises pour lutter contre la propagation du virus COVID-19, le dossier ne peut être retiré sur place. Pour les mêmes raisons, une consultation du dossier et une prise de copie de celui-ci sur place n'est pas non plus possible (article 95 § 2, 3° LCA). Toutes les communications dans ce dossier se feront par ailleurs de manière électronique toujours pour les mêmes raisons.

[8] Art 95, §1er, 8° et 100, §1er, 16° de la loi du 3 décembre 2017 portant création de l'Autorité de protection des données. ; Cf Autorité de protection des données, « Plan Stratégique 2020-2025 », 28 janvier 2020 ; Cf Politique de de publication des décisions de la Chambre contentieuse, 23/12/2020, disponible sur https://www.autoriteprotectiondonnees.be/publications/politique-de-publication-des-decisions-de-la-chambre-contentieuse.pdf.

POUR CES MOTIFS,

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

- **d'ordonner au responsable du traitement**, en vertu de l'article 58.2.c) du RGPD et de l'article 95, § 1er, 5° de la LCA, **de se conformer à la demande du plaignant d'exercer** ses droits, plus précisément **son droit d'accès** (art. 15.1 du RGPD) **et de fournir** au plaignant **les informations demandées** (« *communiquer l'intégralité des donnés dont [le responsable du traitement] dispose en précisant quelles données ont faut l'objet du hacking* ») aussi sur base de l'article 95, § 1er, 6° de la LCA , et ce dans le délai de 14 jours à compter de la notification de la présente décision ;

- **d'ordonner au responsable du traitement d'informer** par e-mail **l'Autorité de protection des données** (Chambre Contentieuse) **du résultat de cette décision** dans le même délai via l'adresse e-mail litigationchamber@apd-gba.be; et

- de **formuler un avertissement** au responsable du traitement en vertu de l'article 58.2.a) du RGPD et de l'article 95, § 1er, 4° de la LCA qu'il se place en porte à faux vis-à-vis du RGPD en cas de non mise en conformité dans l'avenir de son système informatique à son obligation de sécurité

- **si le responsable du traitement 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**.

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.

(Sé). Hielke Hijmans

Président de la Chambre Contentieuse