Chambre Contentieuse

Décision quant au fond 170/2023 du 20 décembre 2023

Numéro de dossier : DOS-2019-04346

Objet : Fuite de données dans le cadre d'un programme de fidélité

La Chambre Contentieuse de l'Autorité de protection des données, constituée de monsieur Hielke HIJMANS, président, et de messieurs Dirk Van Der Kelen et Christophe Boeraeve, membres ;

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 :

La défenderesse : Y, représentée par maître Cédric Burton et maître Laura Brodahl, ci-après "la défenderesse"

I. Faits et procédure

A. Enquête du Service d'Inspection

1. Le 20 décembre 2019, le Comité de direction de l'Autorité de protection des données (ci-après "l'APD") a décidé de saisir le Service d'Inspection de l'APD d'une affaire sur la base de l'article 63, 1° de la LCA, considérant qu'il semblait y avoir des indices sérieux que la défenderesse ne respectait pas les obligations découlant de l'article 32 du RGPD. Les éléments pris en considération à cet égard par le Comité de direction étaient l'ampleur de la fuite de données, le nombre de personnes concernées s'élevant à 89.429, réparties dans 27 États membres de l'UE, ainsi que la nature des données ayant été divulguées, à savoir le numéro de carte, le nom de la personne concernée, sa date de naissance, son sexe, son adresse, son adresse e-mail, son numéro de téléphone, son numéro de GSM et un numéro d'identification unique.

2. Suite au traitement par le Secrétariat Général de l'APD de la fuite de données survenue auprès de la défenderesse le 19 août 2019 et aux plaintes introduites auprès du Service de Première Ligne de l'APD par des personnes en Allemagne en leur qualité de personnes concernées touchées par la fuite de données, le dossier a été examiné par le Secrétariat Général et transmis au Comité de direction en vertu de l'article 63, 1° de la LCA, en vue de saisir le Service d'Inspection, et les plaintes individuelles des citoyens allemands, après avoir été déclarées recevables par le Service de Première Ligne, ont également été transmises au Service d'Inspection en vertu de l'article 96, § 1er de la LCA *juncto* l'article 63, 2° de la LCA.

3. Le motif de la saisine susmentionnée était une fuite de données concrète au niveau d'un sous-traitant de la défenderesse. Ce sous-traitant gère la plate-forme du programme (..) sur laquelle les titulaires de carte peuvent s'inscrire à un programme de fidélité basé sur des points qu'ils obtiennent en utilisant leur carte pour effectuer des achats. Cette plate-forme permettait aux titulaires de carte d'accéder à leurs données, y compris leur solde de points, et de les utiliser ensuite pour bénéficier de promotions proposées par les commerçants participants qui affichaient leurs offres sur la plate-forme. Le sous-traitant a fait lui-même appel à son tour à un sous-traitant pour l'hébergement/la journalisation externes.

4. Le 20 juillet 2023 l'enquête du Service d'Inspection est clôturée, le rapport est joint au dossier et celui-ci est transmis par l'Inspecteur général au Président de la Chambre Contentieuse (art. 91, § 1er et § 2 de la LCA), ce qui a donné lieu à la saisine de la Chambre Contentieuse en vertu de l'article 92, 3° de la LCA. Dans son rapport, le Service d'Inspection était arrivé à la conclusion que le grand nombre de personnes concernées touchées par la fuite de données et le respect de l'obligation de notification à l'APD ne suffisaient pas en soi pour conclure à l'existence d'un indice d'une pratique susceptible de donner lieu à une

violation des principes fondamentaux de la protection des données à caractère personnel au sens de l'article 63, 1° de la LCA. Pour le reste, le rapport d'inspection ne comporte aucune constatation d'une quelconque violation du RGPD dans le chef de la défenderesse.

B. Procédure devant la Chambre Contentieuse

5. Le 27 septembre 2023 la Chambre Contentieuse décide, en vertu de l'article 95, § 1er, 1° et de l'article 98 de la LCA, que le dossier peut être traité sur le fond. La défenderesse est informée par envoi recommandé des dispositions telles que reprises à l'article 95, § 2 ainsi qu'à l'article 98 de la LCA. Elle est également informée, en vertu de l'article 99 de la LCA, du délai pour transmettre la conclusion. La date limite pour la réception des conclusions en réponse de la défenderesse a été fixée initialement au 30 octobre 2023, mais a été prolongée au 15 novembre 2023.
6. Le 6 octobre 2023, la défenderesse demande une copie du dossier (art. 95, §2, 3° LCA), laquelle lui est transmise le 18 octobre 2023, et complétée le 25 octobre 2023. La défenderesse accepte également de recevoir toutes les communications relatives à l'affaire par voie électronique, ce conformément à l'article 98 de la LCA.
7. Le 10 novembre 2023, les parties sont informées du fait que l'audition aura lieu le 1er décembre 2023.
8. Le 15 novembre 2023, la Chambre Contentieuse reçoit les conclusions en réponse de la défenderesse. Outre la défense sur le fond qui concerne principalement le rapport technique du Service d'Inspection, ces conclusions reprennent également quelques moyens de défense procéduraux relatifs à la manière dont le Service d'Inspection a été saisi et a mené l'enquête.
9. Le 1er décembre 2023, la défenderesse est entendue par la Chambre Contentieuse. La défenderesse est donc entendue et a la possibilité d'exposer ses arguments.

Ensuite, l'affaire est délibérée par la Chambre Contentieuse.

10. Le 8 décembre 2023, le procès-verbal de l'audition est soumis à la défenderesse, conformément à l'article 54 du règlement d'ordre intérieur. La défenderesse se voit ainsi offrir l'opportunité de faire ajouter ses éventuelles remarques à cet égard en annexe du procès-verbal, sans que cela implique une réouverture des débats.
11. Le 15 décembre 2023, la Chambre Contentieuse reçoit quelques remarques relatives au procès-verbal qu'elle décide de reprendre dans sa délibération.

II. Motivation

A. Procédure

12. La défenderesse fait valoir qu'une enquête du Comité de Direction ou du Service d'Inspection ne peut être ouverte de leur propre initiative que s'il existe des indices sérieux de défaut de conformité. Selon la défenderesse, aucun de ces deux organes n'a établi l'existence de tels indices. Ils auraient par conséquent tous les deux illégalement mené une enquête relative aux activités de traitement de la défenderesse.

13. À cet égard, la Chambre Contentieuse se doit de faire remarquer que la note adressée par le Secrétariat Général au Comité de direction suite à la notification de la fuite de donnée par la défenderesse, laquelle a servi de base à la décision du Comité de direction de transmettre le dossier au Service d'Inspection, mentionne clairement que des éléments suffisants dans la note indiquent une pratique qui entraîne une violation des principes fondamentaux de la protection des données à caractère personnel (article 63, 1° de la LCA). La note en question souligne explicitement le grand nombre de personnes concernées touchées par cette fuite de données, réparties dans 27 États membres de l'UE. La note pointe également que l'APD a déjà reçu sept plaintes de citoyens allemands et que l'autorité de contrôle du Länder allemand de la Hesse a elle-même reçu environ trois cents plaintes concernant cette fuite de données qui pourraient encore être transférées à l'APD.

14. La Chambre Contentieuse constate que sur la base de la note, il existait bel et bien des indices sérieux pouvant indiquer une pratique entraînant des violations de la protection des données. Dans ce contexte, il s'agissait de prendre en compte non seulement l'impact de la fuite de données sur le grand nombre de personnes concernées, mais aussi la nature des données, qui consistaient potentiellement en des données financières. Selon la Chambre Contentieuse, ces indices constituaient au moins une justification suffisante pour examiner si la déclaration de la défenderesse, telle que mentionnée dans la note, selon laquelle le réseau de paiements est séparé de la plate-forme où sont rassemblées les données à caractère personnel des clients dans le cadre du programme (..) était exacte.

15. Évidemment, ce n'est qu'après une enquête par le Service d'Inspection qu'il peut être établi que, le cas échéant, il n'y a pas de pratique au sens de l'article 63, 1° de la LCA. Cette constatation du Service d'Inspection ne porte pas préjudice à la licéité de la décision du Comité de direction selon laquelle, sur la base des éléments disponibles à ce moment-là et donc avant l'enquête du Service d'Inspection, il existait des indices sérieux requérant une enquête par le Service d'Inspection. La Chambre Contentieuse estime dès lors que le Service d'Inspection a été saisi en conformité avec l'article 63, 1° de la LCA et a valablement mené son enquête.

16. La défenderesse fait en outre valoir que l'APD ne formule aucune allégation de défaut de conformité. La défenderesse se réfère pour cela au rapport d'inspection dans lequel aucune violation n'a été constatée, ainsi qu'au courrier de la Chambre Contentieuse dans lequel la défenderesse est invitée à commenter les mesures qu'elle a prises, conformément aux articles 24 et suivants du RGPD.

17. La Chambre Contentieuse explique qu'il est établi qu'une fuite de donnée s'est produite en 2019, mais que dans sa décision, elle souhaite tenir compte de l'évolution intervenue entre-temps afin d'obtenir une vue globale de la situation actuelle pour parvenir à un avis équilibré. C'est uniquement dans cette perspective que la Chambre Contentieuse a procédé à l'examen de cette affaire quant au fond et que, dans le cadre de cette procédure, elle a demandé à la défenderesse de fournir des explications sur les mesures techniques et organisationnelles prises.

B. Mesures techniques et organisationnelles

18. Selon les informations soumises par celle-ci, dès la prise de connaissance de la fuite de données, la défenderesse a immédiatement suspendu le site web du programme (..) et a retiré tous les accès aux données stockées sur la plateforme. La défenderesse a évalué l'impact de l'incident et a conclu qu'il n'a pas entraîné de risque élevé pour les personnes. L'incident était limité au programme et n'a en aucun cas impacté le réseau de paiement de la défenderesse. Néanmoins, par excès de prudence, la défenderesse a également informé les personnes concernées le 22 août 2019 afin qu'elles puissent prendre d'éventuelles mesures de précaution, si celles-ci s'avéraient nécessaires.

19. En ce qui concerne la fuite de données qui a donné lieu à la présente décision, la Chambre Contentieuse se doit dès lors de constater que la défenderesse a notifié cette fuite de données à l'APD dans le cadre prescrit par l'article 33 du RGPD, malgré que la fuite de données ait été évaluée par la défenderesse comme présentant peu de risques pour les personnes concernées. En ce qui concerne concrètement la notification de la fuite de données à l'APD, la défenderesse a agi en conformité avec le RGPD.

20. En outre, les éléments factuels du dossier montrent qu'il n'y a pas eu de fuites de données répétées indiquant des défaillances systématiques dans le chef de la défenderesse suite auxquelles elle aurait manqué aux obligations imposées par l'article 24 *juncto* l'article 32 du RGPD. La fuite de données constitue au contraire un fait totalement isolé.

21. Par ailleurs, les documents versés au dossier par la défenderesse ont permis à la Chambre Contentieuse de comprendre en profondeur l'approche prospective de la défenderesse afin d'éviter une répétition des faits tels qu'ils se sont produits. Ces mesures ont fait l'objet d'une évaluation par la Chambre Contentieuse, qui est parvenue aux conclusions suivantes.

22. La défenderesse continue de développer avec succès ses processus à l'égard des fournisseurs. Ces développements comprennent un certain nombre d'initiatives qui vont au-delà des exigences légales. Dans le contexte de son engagement d'assurer une sécurité continue, la défenderesse revoit et améliore ses mesures de sécurité des données en tenant compte des progrès technologiques disponibles sur le marché, et en suivant "l'état de l'art" qui est en constante évolution. En particulier, la défenderesse :

    - a mis à jour ses questionnaires de due diligence à l'égard des fournisseurs ainsi que ses politiques et processus d'évaluation des risques liés aux fournisseurs ;
    - a réalisé des audits des fournisseurs actifs en Europe ;
    - a effectué une vérification des certifications des fournisseurs actifs en Europe ;
    - a fourni des formations à des employés de différents services sur les rôles et les responsabilités en matière de gestion des risques liés aux fournisseurs ;
    - a immédiatement intégré le programme de gestion des fournisseurs dans les autres processus de la société ;
    - a ajouté un nouveau niveau de risque à son modèle d'évaluation des risques ;
    - a mis à jour ses outils de suivi pour rendre ce contrôle et le suivi des fournisseurs plus efficace et les outils plus souples à gérer ;
    - a agrandi son équipe chargée des évaluations des fournisseurs ;
    - a mis à jour son questionnaire de réévaluation ;
    - a mis en place une nouvelle liste standardisée de mesures de sécurité à laquelle tous les fournisseurs doivent se conformer ;
    - a affiné son processus d'évaluation du risque afin de répartir les ressources entre départements de manière plus efficace ; et
    - assure une sensibilisation permanente au programme à l'égard des fournisseurs, y compris par la formation des cadres et l'implication du plus haut niveau de gestion ; et en communiquant largement l'adresse courriel aux *Business Owners* afin qu'ils puissent aisément contacter l'équipe pour obtenir de l'aide ou en cas de problèmes avec les fournisseurs.

23. Il ressort de l'ensemble de ces éléments que (i) la défenderesse a rapidement fait le nécessaire dès la survenance de la fuite de données ; (ii) le Service d'Inspection n'a pas fait de constatation indiquant qu'une violation aurait été commise dans le chef de la défenderesse ; (iii) la défenderesse a démontré de manière circonstanciée que des mesures approfondies avaient été prises et que ces mesures sont soumises à une actualisation

permanente afin de prévenir de tels faits à l'avenir. Ceci amène la Chambre Contentieuse à conclure qu'**aucune violation** du RGPD n'a été commise dans le chef de la défenderesse.

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. Conformément à sa *Politique en matière de publication de ses décisions*[1], la Chambre Contentieuse publie chacune de ses décisions dans un objectif de transparence administrative, laquelle transparence est requise tant au titre de ses missions comme autorité de contrôle de protection des données (article 57.1. b) et d) lu conjointement avec l'article 51 du RGPD) que de sa qualité d'autorité administrative soumise aux principes de bonne administration. C'est à ce titre que la présente décision est publiée.

25. Toutefois, il n'est pas nécessaire à cette fin que les données d'identification des parties soient directement communiquées

26. En outre, pour parvenir à la décision relative à la publication, il a également été tenu compte du fait que sept plaintes avaient été introduites par des citoyens allemands souhaitant savoir quelles mesures de sécurité avaient été prises par la défenderesse afin de prévenir les fuites de données. Ces plaintes sont en lien direct avec la fuite de données faisant l'objet de la présente décision. Ces plaignants ont non seulement droit à une décision de la Chambre Contentieuse qui doit nécessairement reprendre les mêmes considérations que dans la présente décision mais en outre, on ne peut ignorer le fait que de par la nature des faits à la base de leur plainte et qui visent la défenderesse dans la présente décision, les plaignants ont connaissance de l'identité de la défenderesse. La Chambre Contentieuse n'a toutefois pas le pouvoir d'interdire à ces plaignants de faire connaître la décision prise par la Chambre Contentieuse ni d'en interdire la publication. C'est pourquoi la Chambre Contentieuse estime qu'il n'est pas possible d'accéder à la demande de la défenderesse de ne pas procéder à la publication en raison du fait que la publication de la présente décision pourrait potentiellement affecter la défenderesse dans son fonctionnement quotidien par un afflux de questions de clients auraient été alarmés à tort.

27. La Chambre Contentieuse estime toutefois que la présente décision démontre par contre que la défenderesse a tout mis en œuvre pour réaliser le traitement des données à caractère personnel des clients en conformité avec le RGPD, en particulier en ce qui concerne la sécurité des données, et constitue un exemple pour son secteur d'activité pour ce qui concerne la protection des données ainsi que l'attention et les actions continues prises pour s'adapter en permanence aux évolutions dans ce domaine.

---

[1] Autorité de protection des données, Chambre Contentieuse, Politique de publication des décisions de la Chambre contentieuse du 23 décembre 2020 : https://www.autoriteprotectiondonnees.be/publications/politique-de-publication-des-decisions-de-la-chambre-contentieuse.pdf

PAR CES MOTIFS,

la Chambre Contentieuse de l'Autorité de protection des données décide, après délibération, de classer la présente plainte sans suite en vertu de l'article 100, § 1er, 1° de la LCA, étant donné qu'aucune violation du RGPD ne peut être constatée à cet égard.

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[2]. La requête interlocutoire doit être déposée au greffe de la Cour des Marchés conformément à l'article 1034*quinquies* du C. jud.[3], ou via le système d'information e-Deposit du Ministère de la Justice (article 32*ter* du C. jud.).

(sé). Hielke HIJMANS

Président de la Chambre Contentieuse

[2] 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.

[3] 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.