Autorité de protection des données
Gegevensbeschermingsautoriteit

Chambre Contentieuse

Décision quant au fond 129/2022 du 23 août 2022

Numéro de dossier : DOS-2020-01079

Objet : Plainte pour défaut de niveau de protection suffisant dans le cadre des traitements de données à caractère personnel

La Chambre Contentieuse de l'Autorité de protection des données, constituée de Monsieur Hielke Hijmans, président, et de Messieurs Dirk Van Der Kelen et Jelle Stassijns, 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 "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 : Monsieur X, ci-après "le plaignant" ;

Le défendeur : Y, ci-après "le défendeur"

I. Faits et procédure

1. Le 3 avril 2020, le plaignant a porté plainte auprès de l'Autorité de protection des données (ci-après "APD") contre le défendeur.

2. La plainte concerne le fait que des documents personnels du plaignant ont été mis automatiquement à la disposition d'un tiers. Le plaignant pratique le cohousing avec un ami, un tiers dans la présente procédure. Dans le cadre de ce cohousing, il a été convenu entre le plaignant et le tiers que ce dernier chargerait la facture commune d'eau, au nom du plaignant, sur son compte Y personnel. Y est une plateforme sur laquelle un utilisateur peut gérer son administration, comme une archive numérique. L'utilisateur peut ainsi charger et gérer des documents personnels, comme des factures, effectuer des paiements, etc. Le chargement de la facture d'eau au nom du plaignant a eu pour conséquence que la plateforme Y a proposé automatiquement au tiers d'ajouter à son compte d'autres documents au nom du plaignant, émis par d'autres entreprises auprès desquelles le plaignant est client. Ces nouvelles connexions proposées ont été refusées par le tiers. À la demande du Service de Première Ligne, le plaignant a pris contact avec le défendeur. Le défendeur a indiqué être disposé à résoudre ce problème. Le plaignant a introduit la plainte contre la situation qui existait avant les adaptations techniques sur la plateforme Y, telles qu'apportées par le défendeur.

3. Le 30 avril 2020, la plainte est déclarée recevable par le Service de Première Ligne sur la base des articles 58 et 60 de la LCA et la plainte est transmise à la Chambre Contentieuse en vertu de l'article 62, § 1er de la LCA.

4. Le 11 août 2020, les parties concernées sont informées par envoi recommandé des dispositions visées à l'article 95, § 2 ainsi qu'à l'article 98 de la LCA. Les parties concernées sont également informées, en vertu de l'article 99 de la LCA, des délais pour transmettre leurs conclusions.

   La date limite pour la réception des conclusions en réponse du défendeur a été fixée au 13 octobre 2020, celle pour les conclusions en réplique du plaignant au 3 novembre 2020 et celle pour les conclusions en réplique du défendeur au 24 novembre 2020.

5. Le 12 août 2020, le défendeur accepte toutes communications relatives à l'affaire par voie électronique.

6. Le 17 août 2020, le plaignant accepte toutes communications relatives à l'affaire par voie électronique.

7. Le 7 octobre 2020, la Chambre Contentieuse reçoit les conclusions en réponse de la part du défendeur. Le défendeur insiste sur le fait qu'un compte d'utilisateur chez Y est personnel, le but étant qu'un utilisateur ajoute à son propre compte uniquement des documents à son nom. Étant donné que le tiers a chargé la facture d'eau (au nom du plaignant), Y a proposé deux nouvelles connexions. Le défendeur explique que ces connexions peuvent être considérées comme un

dossier dans lequel des documents sont conservés pour un utilisateur final d'une entreprise déterminée. Ce dossier est seulement complété par des documents et informations lorsqu'une connexion est établie avec cette entreprise. Lorsque ces deux connexions ont été proposées au tiers, il n'y avait donc pas d'accès aux documents proprement dits. Toutefois, sur la base de ces nouvelles propositions, le tiers pouvait déduire que le plaignant était client de ces deux entreprises. Ensuite, le défendeur souligne que l'incident a été résolu dans les 48 heures. Enfin, le défendeur formule quelques propositions d'amélioration qui seraient implémentées dans les six mois sur la plateforme :

- une meilleure information quant aux effets de l'ajout d'une connexion ;
- une meilleure information quant au caractère personnel du compte d'utilisateur.

8. Le 9 octobre 2020, la Chambre Contentieuse reçoit les conclusions en réplique de la part du plaignant. Le plaignant renvoie aux conclusions en réponse du défendeur qui affirment qu'un compte Y est personnel. Le plaignant souligne qu'il n'a pas de compte et qu'il estime donc que cela n'est pas pertinent. Ensuite, le plaignant avance que la plateforme Y est entachée de quelques erreurs de conception fondamentales et illégales. Le tiers a en effet pu introduire une facture au nom du plaignant, ce qui implique en outre que de nouvelles connexions sont proposées, permettant au tiers d'accéder à encore plus de données à caractère personnel du plaignant. Le plaignant n'a pas non plus été informé d'une quelconque manière, ni consulté ou averti à cet égard. Le plaignant souligne également que les documents des nouvelles connexions n'ont pas été ajoutés au compte Y du tiers, mais que le tiers a bien déclaré formellement qu'il pouvait les consulter. Le fait que les documents n'ont pas été consultés résulte dès lors de l'attitude bien intentionnée du tiers et non des mesures de sécurité nécessaires de la plateforme, selon le plaignant.

9. Le 24 novembre 2020, la Chambre Contentieuse reçoit les conclusions en réplique du défendeur. Le défendeur insiste sur le fait que le caractère personnel du compte d'utilisateur est bien pertinent en raison de la combinaison de mesures qu'Y prend et des fonctionnalités qu'Y propose. La bonne utilisation de la plateforme Y est en effet de ne pas ajouter des documents d'autres personnes à son propre compte. Ensuite, le défendeur souligne qu'il n'y a aucune erreur de conception fondamentale et illégale dans la plateforme. Selon le défendeur, cette plainte est la conséquence d'un accord entre le plaignant et le tiers. Le plaignant a donné son autorisation au tiers pour ajouter la facture d'eau, au nom du plaignant, au compte d'utilisateur du tiers sur la plateforme Y. Pour ajouter ce document, le tiers a eu accès aux données personnelles du plaignant, à savoir son numéro de client et le code de sécurité sur la facture de son fournisseur d'eau. Sans ces données, le tiers ne pouvait pas ajouter la facture à son compte d'utilisateur. Le défendeur souligne qu'Y n'a aucun contrôle sur la communication entre fournisseur et client, comme des factures ou autres communications confidentielles. Le défendeur n'a pas accès à ces données et n'a aucune influence sur la manière dont le fournisseur et le client traitent ces données.

10. Le plaignant a indiqué dans ses conclusions qu'il n'a été ni informé ni averti que de (nouvelles) connexions seraient établies. Le défendeur indique dans ses conclusions que le plaignant n'est pas un utilisateur de la plateforme Y et que de ce fait, le défendeur ne disposait pas de ses données à caractère personnel pour avertir le plaignant. Enfin, le défendeur souhaite réfuter que le tiers a eu accès aux documents dans les nouvelles connexions précitées. Le défendeur argumente que les documents ne sont visibles pour un utilisateur que lorsqu'il les a ajoutés via l'introduction d'un code de sécurité ou l'acceptation d'une invitation. Sans ce code ou cette invitation, aucun document n'est ajouté à un compte d'un utilisateur et il ne peut donc pas y avoir d'accès à ces documents. Les journalisations d'Y démontrent que le tiers n'a pas accepté l'invitation à une nouvelle connexion et que dès lors, aucun document n'a été ajouté et qu'une consultation était donc impossible. Le défendeur affirme en outre se montrer constructif et indique qu'il mettra en œuvre une fonctionnalité supplémentaire dans un délai de six mois, à savoir une sécurité supplémentaire avec l'eID et/ou Itsme. Un contrôle supplémentaire est ainsi créé concernant l'identité de l'utilisateur.

11. Le 25 mai 2022, le défendeur est informé du fait que l'audition aura lieu le 21 juin 2022.

12. Le 21 juin 2022, les parties sont entendues par la Chambre Contentieuse et ont ainsi l'occasion d'avancer leurs arguments. Le plaignant a comparu en personne et le défendeur a comparu par l'intermédiaire du CEO et de son avocat. Ensuite, l'affaire est délibérée par la Chambre Contentieuse.

13. Le 27 juin 2022, le procès-verbal de l'audition est transmis aux parties, conformément à l'article 54 du règlement d'ordre intérieur de l'APD. Les parties se voient ainsi offrir l'opportunité de faire ajouter leurs éventuelles remarques à cet égard en annexe du procès-verbal, sans que cela implique une réouverture des débats.

14. Le 4 juillet 2022, la Chambre Contentieuse reçoit du plaignant quelques remarques relatives au procès-verbal qu'elle décide de reprendre dans sa délibération.

15. Le 5 juillet 2022, la Chambre Contentieuse reçoit de la part du défendeur la communication qu'il n'a pas de remarque à formuler au sujet du procès-verbal.

16. Le 6 juillet 2022, la Chambre Contentieuse fait connaître au défendeur son intention de procéder à l'imposition d'une amende administrative ainsi que le montant de celle-ci, afin de donner au défendeur l'occasion de se défendre avant que la sanction soit effectivement infligée.

17. Le 12 juillet 2022, la Chambre Contentieuse reçoit la réaction du défendeur concernant l'intention d'infliger une amende administrative, ainsi que le montant de celle-ci. Le défendeur ne souhaite pas formuler de remarques à cet égard.

II. Motivation

Article 5.1.f) du RGPD, article 5, paragraphe 2 du RGPD, article 24, paragraphe 1 du RGPD et article 32, paragraphes 1 et 2 du RGPD concernant la vérification de l'identité

18. L'article 5.1.f) du RGPD prescrit que les données à caractère personnel doivent être "*traitées de façon à garantir une sécurité appropriée des données à caractère personnel, 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*".

19. Dans le prolongement de l'article 5, paragraphe 1, f) du RGPD, l'article 32, paragraphe 1 du RGPD dispose que le défendeur, en tant que responsable du traitement, doit mettre en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque. À cet égard, il faut tenir compte de l'état de la technique, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que de la probabilité et de la gravité des risques que présente le traitement pour les droits et libertés des personnes.

20. L'article 32, paragraphe 1 du RGPD dispose que lors de l'évaluation du niveau de sécurité approprié, il faut tenir compte en particulier des risques que présente le traitement, résultant notamment de la destruction, de la perte, de l'altération, de la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou de l'accès non autorisé à de telles données, de manière accidentelle ou illicite.

21. La Chambre Contentieuse rappelle qu'en vertu de l'article 5, paragraphe 2, de l'article 24 et de l'article 32, paragraphes 1 et 2 du RGPD, le principe de responsabilité implique que le responsable du traitement prenne les mesures techniques et organisationnelles nécessaires afin de garantir que le traitement soit conforme au RGPD. L'obligation susmentionnée relève de la bonne exécution de la responsabilité du défendeur, conformément à l'article 5, paragraphe 2, à l'article 24 et à l'article 32 du RGPD. La Chambre Contentieuse souligne que la responsabilité visée à l'article 5, paragraphe 2 et à l'article 24 du RGPD constitue un des piliers centraux du RGPD. Cela implique que le responsable du traitement a la responsabilité, d'une part, de prendre des mesures proactives afin de garantir le respect des prescriptions du RGPD et d'autre part, de pouvoir prouver qu'il a pris de telles mesures.

22. La première étape pour définir le niveau de sécurité approprié du traitement de données à caractère personnel est de cerner les risques de ce traitement et d'en établir une pondération. Sur cette base, il convient de déterminer quelles mesures sont nécessaires pour prévoir une sécurité suffisante contre ces risques. Il résulte du RGPD que pour la pondération des risques en matière de sécurité des données, il convient de prêter attention aux risques qui peuvent survenir lors du traitement de données à caractère personnel, comme la divulgation non autorisée ou l'accès non autorisé aux données traitées. Lors de l'inventaire et de l'évaluation des risques, ce sont surtout

les conséquences d'un traitement illicite de données à caractère personnel que les personnes peuvent subir qui sont pertinentes. Selon que les données ont un caractère plus sensible, ou si le contexte dans lequel celles-ci sont utilisées représente une menace plus importante pour la vie privée, des exigences plus strictes sont posées pour la sécurité des données à caractère personnel.

23. Comme déjà indiqué précédemment, la plateforme Y est une plateforme sur laquelle un utilisateur peut gérer son administration et est comparable à une archive numérique. Ainsi, l'utilisateur peut charger et gérer des documents personnels, comme des factures, effectuer des paiements, etc. La Chambre Contentieuse comprend des conclusions du défendeur qu'un compte a été créé sur la plateforme par un utilisateur et est également géré à son nom (ou au nom de membres de sa famille). L'utilisateur peut désigner des entreprises (fournisseurs) dont il souhaite recevoir les documents administratifs et il peut, moyennant la réalisation des étapes requises, les ajouter à son compte. Vu la nature des entreprises avec lesquelles le responsable du traitement collabore et le grand nombre de fournisseurs qui utilisent la plateforme Y, la Chambre Contentieuse constate que des données à caractère personnel d'utilisateurs de la plateforme sont partagées à grande échelle et qu'il s'agit (pour la plupart) de données sensibles, comme des données traitées notamment par des banques et des mutualités. La nature sensible de ces données doit être prise en compte dans la pondération précitée des risques, le niveau de sécurité devant ainsi y être adapté.

24. La Chambre Contentieuse comprend des conclusions du défendeur que lors de l'utilisation de la plateforme Y, le but n'est pas en principe d'ajouter des factures au nom d'une autre personne dans un compte d'utilisateur personnel. À cet effet, le défendeur prévoit un code de sécurité qui doit être introduit lors de l'ajout de la facture au compte. La Chambre Contentieuse constate toutefois que le défendeur avance lui-même dans ses conclusions qu'il ne contrôle pas la communication entre le fournisseur et le client, ni ce qu'il advient de cette communication. Cela implique qu'en cas de perte ou d'usage impropre du code de sécurité en question, le défendeur ne dispose d'aucun moyen de vérifier si ce code est utilisé de manière licite.

25. La Chambre Contentieuse estime dès lors que le défendeur n'a pas prévu les mesures de sécurité suffisantes, de manière à ce qu'en cas de perte ou d'usage abusif de la communication précitée entre le fournisseur et le client, les données à caractère personnel du client restent protégées. Comme déjà mentionné ci-avant, un tiers peut alors dans ce cas consulter différentes données financières et médicales de la personne concernée par un usage abusif, ce qui ne peut être le but. En outre, comme le constate la Chambre Contentieuse, il est possible qu'en ajoutant une seule facture, plusieurs nouvelles connexions soient établies automatiquement. Une vérification de l'identité de la personne qui utilise le code de sécurité empêcherait que des documents soient ajoutés au compte des mauvaises personnes concernées. Dès lors, la Chambre Contentieuse estime qu'une vérification supplémentaire offrirait une solution plus sûre.

26. La Chambre Contentieuse renvoie aux conclusions de synthèse du défendeur dans lesquelles il affirme qu'il souhaite améliorer le fonctionnement de sa plateforme, en fonction des remarques du plaignant. Il aurait ainsi l'intention de prendre des initiatives dans les six mois pour mieux informer les personnes concernées quant aux conséquences de l'ajout d'une connexion d'une part, et quant au caractère personnel du compte d'utilisateur d'autre part.

27. Le défendeur indique également qu'il prévoira dans un délai de six mois une sécurité supplémentaire au moyen d'une vérification en deux étapes via une identification par le biais de l'eID ou d'Itsme lors de laquelle la personne concernée peut confirmer qu'elle souhaite en effet ajouter ces factures à son compte.

28. Lors de l'audition, le défendeur explique les étapes concrètes qui ont été entreprises au niveau de la mise en place de mesures techniques et organisationnelles dans le cadre de l'établissement d'un niveau de sécurité approprié en vue de la protection des données à caractère personnel.

29. Le défendeur explique que 3 améliorations ont été apportées suite à la plainte :

    a. l'utilisateur est mieux informé au sujet du compte et de son caractère personnel ainsi qu'au sujet du code de sécurité et de son utilisation personnelle ;

    b. l'utilisateur est mieux informé de l'établissement des connexions et des conséquences de celles-ci ; et

    c. une validation supplémentaire via une vérification à deux facteurs du compte bancaire a été mise en œuvre pour garantir l'identité de la bonne personne concernée.

    En outre, le défendeur argumente que plus aucune nouvelle connexion n'est proposée.

30. La Chambre Contentieuse constate que, bien que le défendeur ait mis en œuvre à ce jour la vérification supplémentaire à deux facteurs, un niveau de sécurité insuffisant a existé précédemment lors de l'établissement de connexions. À cet égard, la Chambre Contentieuse évoque le caractère sensible des données qui n'étaient pas suffisamment protégées. La Chambre Contentieuse tient également compte du fait que le défendeur a résolu cela rapidement après la notification du problème de sécurité.

31. Vu ce qui précède, la Chambre Contentieuse estime qu'il est question d'une **violation de l'article 5, paragraphe 1, f) du RGPD, de l'article 5, paragraphe 2 du RGPD, de l'article 24, paragraphe 1 du RGPD et de l'article 32, paragraphes 1 et 2 du RGPD**, étant donné que d'une part, le défendeur n'avait pas pris suffisamment de mesures techniques et organisationnelles pour assurer un niveau de sécurité adapté au risque et que d'autre part, il n'a pas tenu suffisamment compte des risques du traitement lors de la détermination des risques en vue de la sécurité appropriée, en particulier en cas de perte ou d'utilisation illicite.

III. Sanctions

32. La Chambre Contentieuse estime que la violation de l'article 5, paragraphe 1, f), de l'article 5, paragraphe 2, de l'article 24, paragraphe 1 et de l'article 32, paragraphes 1 et 2 du RGPD est avérée, étant donné que le défendeur n'a pas pris suffisamment de précautions pour éviter de potentielles fuites de données.

33. La Chambre Contentieuse estime approprié d'infliger une amende administrative d'un montant de 2.500 euros (article 83, paragraphe 2 du RGPD ; article 100, § 1er, 13° de la LCA et article 101 de la LCA).

34. Vu l'article 83 du RGPD et la jurisprudence[1] de la Cour des marchés, la Chambre Contentieuse motive l'imposition d'une sanction administrative de manière concrète:

    a. la gravité de la violation — il s'agit de l'absence de mesures techniques et organisationnelles pour garantir un niveau de sécurité adapté au risque par une entreprise dont l'activité centrale est le traitement de données à caractère personnel (sensibles) ;

    b. la durée de la violation — la violation n'a pas été remarquée par le défendeur lui-même ; mais après une plainte à cet égard, le problème a été rapidement résolu ;

    c. la résolution de la violation – le défendeur a fait preuve d'une attitude constructive et a pu résoudre la violation dans un bref délai.

35. L'ensemble des éléments exposés ci-dessus justifie une sanction effective, proportionnée et dissuasive, telle que visée à l'article 83 du RGPD, compte tenu des critères d'appréciation qu'il contient. La Chambre Contentieuse souligne qu'en l'espèce, les autres critères de l'article 83, paragraphe 2 du RGPD ne sont pas de nature à donner lieu à une autre amende administrative que celle fixée par la Chambre Contentieuse dans le cadre de la présente décision.

36. De plus, la Chambre Contentieuse attire également l'attention sur les lignes directrices relatives au calcul des amendes administratives *(Guidelines 04/2022 on the calculation of administrative fines under the GDPR*) que l'EDPB a publiées sur son site Internet le 16 mai 2022, pour consultation. Étant donné que ces lignes directrices ne sont pas encore définitives, la Chambre Contentieuse a décidé de ne pas encore en tenir compte pour déterminer le montant de l'amende dans la présente procédure.

37. Les faits, circonstances et violations constaté(e)s justifient dès lors une amende qui sanctionne le défendeur, de sorte que des pratiques entraînant de telles violations ne se reproduisent plus.

[1] Cour d'appel de Bruxelles (section Cour des marchés), *X c. APD,* Arrêt 2020/1471 du 19 février 2020.

IV. Publication de la décision

38. 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, après délibération :

- en vertu de l'article 83 du RGPD et des articles 100, § 1er, 13° et 101 de la LCA, d'infliger au défendeur une amende administrative de 2.500 euros pour violation de l'article 5.1.f), de l'article 5.2, de l'article 24, paragraphe 1 et de l'article 32, paragraphes 1 et 2 du RGPD.

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.

Un tel recours peut être introduit au moyen d'une requête contradictoire qui doit comporter les mentions énumérées à l'article 1034*ter* du *Code judiciaire*[2]. La requête contradictoire doit être déposée au greffe de la Cour des marchés conformément à l'article 1034*quinquies* du *Code judiciaire*[3], ou via le système informatique e-Deposit du Ministère de la Justice (article *32*ter du *Code judiciaire*).

(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.