Autorité de protection des données
Gegevensbeschermingsautoriteit

Chambre Contentieuse

Décision quant au fond 05/2021 du 22 janvier 2021

Numéro de dossier : DOS-2019-04867

Objet : plainte pour attribution du numéro de téléphone du plaignant à un tiers

La Chambre Contentieuse de l'Autorité de protection des données, constituée de Monsieur Hielke Hijmans, président, et de Messieurs Jelle Stassijns et Frank De Smet, 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 :

- le plaignant : Monsieur X

- le défendeur : Y

1. Faits et procédure

1. Le 20 septembre 2019, le plaignant a porté plainte auprès de l'Autorité de protection des données contre Y. La plainte a été déclarée recevable par le Service de première ligne le 30 septembre 2019. La plainte concerne l'attribution présumée du numéro de téléphone portable du plaignant par son fournisseur Y à un tiers, avec pour effet que le plaignant ne pouvait plus disposer de son numéro. La carte SIM du plaignant a été désactivée et le tiers aurait donc pu avoir connaissance du trafic et des appels passés par le plaignant sur son GSM personnel, ainsi que des comptes associés (tels que Paypal, WhatsApp et Facebook) du 16 au 19 septembre 2019 inclus.

2. Vu que la plainte est adressée contre Y dont le siège principal se situe dans l'État membre Z, l'Autorité de protection des données a pris contact avec le contrôleur de cet État membre afin de vérifier si la plainte devait ou non être considérée comme transfrontalière. Cette communication a mené à un examen de la plainte et du traitement de données selon la procédure nationale de l'Autorité belge de protection des données (art. 56.2 du RGPD)[1], avec Y comme défendeur.

3. Le 15 avril 2020, la Chambre Contentieuse a décidé que la plainte pouvait être examinée sur le fond et a informé sans délai le plaignant et le défendeur de cette décision par envoi recommandé. De même, les parties ont été informées des dispositions de l'article 98 de la LCA ainsi que des délais pour introduire leurs conclusions. La date limite pour la réception des conclusions en réponse du défendeur a été fixée au 27 mai 2020, celle pour les conclusions en réplique du plaignant au 17 juin 2020 et celle pour les conclusions en réplique du défendeur au 8 juillet 2020.

4. Par courrier du 20 avril 2020, les conseils du défendeur se sont identifiés dans le dossier, ont demandé une copie du dossier et ont exprimé leur souhait d'être entendus lors d'une audition sur la base de l'article 98, 2° de la LCA.

5. Le 27 mai 2020, le défendeur a introduit des conclusions en réponse.

6. Ni le plaignant, ni le défendeur n'ont fait usage de la possibilité d'introduire des conclusions en réplique. Le plaignant n'a pas souhaité recourir à la possibilité d'être entendu.

7. Le 9 novembre 2020, le défendeur est entendu par la Chambre Contentieuse, conformément à l'article 53 du règlement d'ordre intérieur.

---

[1] L'article 56.2 prévoit ce qui suit : Par dérogation au paragraphe 1, chaque autorité de contrôle est compétente pour traiter une réclamation introduite auprès d'elle ou une éventuelle violation du présent règlement, si son objet concerne uniquement un établissement dans l'État membre dont elle relève ou affecte sensiblement des personnes concernées dans cet État membre uniquement.

8. Le 19 novembre 2020, le procès-verbal de l'audition est soumis aux parties. Les parties n'y ont pas réagi.

9. Le 7 décembre 2020, l'intention d'infliger une amende est communiquée au défendeur. Le 22 décembre 2020, le défendeur a réagi à cette intention de manière circonstanciée.

2. Base juridique

Article 5.1.f) du RGPD

1. Les données à caractère personnel sont :

f) 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 (intégrité et confidentialité).

Article 5.2 du RGPD

Le responsable du traitement est responsable du respect du paragraphe 1 et est en mesure de démontrer que celui-ci est respecté (responsabilité).

Article 24 du RGPD

1. Compte tenu 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, le responsable du traitement met en œuvre des mesures techniques et organisationnelles appropriées pour s'assurer et être en mesure de démontrer que le traitement est effectué conformément au présent règlement. Ces mesures sont réexaminées et actualisées si nécessaire.

2. Lorsque cela est proportionné au regard des activités de traitement, les mesures visées au paragraphe 1 comprennent la mise en œuvre de politiques appropriées en matière de protection des données par le responsable du traitement.

3. L'application d'un code de conduite approuvé comme le prévoit l'article 40 ou de mécanismes de certification approuvés comme le prévoit l'article 42 peut servir d'élément pour démontrer le respect des obligations incombant au responsable du traitement.

Article 32 du RGPD

1. 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, le responsable du traitement et le sous-traitant mettent en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque, y compris entre autres, selon les besoins :

a) la pseudonymisation et le chiffrement des données à caractère personnel ;

b) des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement

c) des moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique d) une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement.

2. Lors de l'évaluation du niveau de sécurité approprié, il doit être tenu 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.

3. L'application d'un code de conduite approuvé comme le prévoit l'article 40 ou d'un mécanisme de certification approuvé comme le prévoit l'article 42 peut servir d'élément attestant du respect des exigences prévues au paragraphe 1 du présent article.

4. Le responsable du traitement et le sous-traitant doivent prendre des mesures pour garantir que toute personne physique agissant sous l'autorité du responsable du traitement ou sous celle du sous-traitant, qui a accès à des données à caractère personnel, ne les traite pas, excepté sur instruction du responsable du traitement, à moins d'y être obligée par le droit de l'Union ou le droit d'un État membre."

Article 33 du RGPD

1. En cas de violation de données à caractère personnel, le responsable du traitement en notifie la violation en question à l'autorité de contrôle compétente conformément à l'article 55, dans les meilleurs délais et, si possible, 72 heures au plus tard après en avoir pris connaissance, à moins que la violation en question ne soit pas susceptible d'engendrer un risque pour les droits et libertés des personnes physiques. Lorsque la notification à l'autorité de contrôle n'a pas lieu dans les 72 heures, elle est accompagnée des motifs du retard.

2. Le sous-traitant notifie au responsable du traitement toute violation de données à caractère personnel dans les meilleurs délais après en avoir pris connaissance.

3. La notification visée au paragraphe 1 doit, à tout le moins :

a) décrire la nature de la violation de données à caractère personnel y compris, si possible, les catégories et le nombre approximatif de personnes concernées par la violation et les catégories et le nombre approximatif d'enregistrements de données à caractère personnel concernés;
b) le nom et les coordonnées du délégué à la protection des données ou d'un autre point de contact auprès duquel des informations supplémentaires peuvent être obtenues ;
c) décrire les conséquences probables de la violation de données à caractère personnel ;
d) décrire les mesures prises ou que le responsable du traitement propose de prendre pour remédier à la violation de données à caractère personnel, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives.

4. Si, et dans la mesure où, il n'est pas possible de fournir toutes les informations en même temps, les informations peuvent être communiquées de manière échelonnée sans autre retard indu.

5. Le responsable du traitement documente toute violation de données à caractère personnel, en indiquant les faits concernant la violation des données à caractère personnel, ses effets et les mesures prises pour y remédier. La documentation ainsi constituée permet à l'autorité de contrôle de vérifier le respect du présent article."

Article 34.1 du RGPD

34.1. Lorsqu'une violation de données à caractère personnel est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne physique, le responsable du traitement communique la violation de données à caractère personnel à la personne concernée dans les meilleurs délais.

3. Motivation

3.1 Conclusions et analyse de la Chambre Contentieuse

Procédure suivie

10. Le défendeur a réagi à l'intention d'infliger une amende. La réaction implique notamment que le défendeur considère que les droits de la défense ont été violés par la Chambre Contentieuse. Selon le défendeur, les violations constatées par la Chambre Contentieuse sont peu, voire pas liées à la plainte introduite initialement par le plaignant. Le défendeur affirme que dans sa plainte, le plaignant a uniquement déclaré qu'il était question d'une violation de sa vie privée, sans spécifier de quelles violations il s'agissait. Le défendeur estime que la tâche de la Chambre Contentieuse était de qualifier cette plainte juridiquement et d'en aviser immédiatement le défendeur. Le défendeur affirme avoir été informé des violations spécifiques pour la première fois le 7 décembre 2020, donc par le biais de l'intention communiquée d'infliger une amende, et qu'il n'a dès lors pas pu se défendre efficacement contre les accusations. En outre, le défendeur estimait qu'il était nécessaire en l'espèce que la Chambre Contentieuse saisisse le Service d'Inspection. Cela n'a pas eu lieu et après la clôture des débats, la Chambre Contentieuse a qualifié elle-même juridiquement les faits, selon le défendeur.

11. La Chambre Contentieuse souhaite attirer l'attention de manière générale sur le fait que pour les personnes concernées dont les données à caractère personnel sont traitées, l'introduction d'une plainte ne doit pas être compliquée. La procédure de plainte telle que prévue à l'article 77 du RGPD et telle que développée dans la LCA est conçue comme une alternative à un recours aux tribunaux civils ou administratifs. Le droit de plainte auprès de l'APD doit demeurer aisé et accessible pour le citoyen. Ainsi, le législateur n'a par exemple pas voulu que les parties soient toujours assistées par un avocat.[2]
    L'article 60 de la LCA pose des exigences peu élevées à la recevabilité d'une plainte. Pour qu'une plainte soit déclarée recevable, il est seulement requis qu'elle soit rédigée dans une des langues nationales, qu'elle contienne un exposé des faits ainsi que les indications nécessaires pour identifier le traitement sur lequel elle porte et qu'elle relève de la compétence de l'APD. L'article ne prescrit pas que la plainte doive comporter une violation présumée à une disposition légale.

12. Lors de l'évaluation du caractère fondé de la plainte, la Chambre Contentieuse ne vérifiera donc pas si dans la plainte introduite formellement auprès de l'APD, les plaignants ont bien invoqué la bonne disposition légale pour appuyer leur demande, mais bien si les faits en question constituent une atteinte à l'une des dispositions légales dont le respect est soumis au contrôle de l'APD. La Chambre Contentieuse souligne encore à cet égard que le contrôle du respect du RGPD est la mission principale de cet organe de contrôle.

[2] Voir par ex. le Plan de Gestion 2021 de l'APD, p. 18.

13. Dans une décision antérieure, la Chambre Contentieuse a considéré ce qui suit :

"De même, les plaignants ne sont pas tenus d'invoquer tous les faits pertinents concernant l'atteinte alléguée dans leur plainte. La Chambre contentieuse doit pouvoir les aider en posant des questions dirigées de manière à bien comprendre en fait et en droit l'atteinte potentielle à un droit fondamental que le plaignant souhaite porter à son attention. La Chambre contentieuse peut également tenir compte de griefs développés ultérieurement par voie de conclusion par le plaignant pour autant qu'il s'agisse de faits ou arguments juridiques liés à l'atteinte alléguée dont elle a été saisie par voie de plainte, et dans le respect des droits de la défense."

"Durant la procédure consécutive à la plainte, la Chambre contentieuse a donc la possibilité de faire évoluer la qualification juridique des faits qui lui sont soumis, ou examiner de nouveaux faits liés à la plainte, sans nécessairement faire appel à l'intervention du Service d'Inspection, notamment en posant des questions aux parties ou en tenant compte des nouveaux faits ou qualifications invoqués par voie de conclusion, et ce, dans les limites du débat contradictoire, à savoir, pour autant que les parties aient eu l'occasion de débattre de ces faits ou qualifications juridiques de manière conforme aux droits de la défense. Au besoin, il appartient à la Chambre contentieuse de susciter ce débat soit dans sa lettre d'invitation à conclure sur pied de l'article 98 de la LCA, soit ultérieurement dans le cadre d'une réouverture des débats. Dans ce contexte, le fait de tenir compte d'une nouvelle qualification juridique invoquée par le plaignant ne nuit pas au caractère équitable de la procédure et à l'égalité des armes, a fortiori dans la mesure où les décisions de la Chambre contentieuse sont susceptibles d'un appel de pleine juridiction auprès de la Cour des marchés[3]."

14. La Chambre Contentieuse estime - contrairement au défendeur - qu'en l'espèce, le défendeur a pu se défendre entièrement et contre toutes les violations incriminées et qu'il n'a pas été question de nouveaux faits notifiés ultérieurement contre lesquels le défendeur n'a pas pu se défendre. Au moyen des conclusions en réponse introduites le 27 mai 2020, le défendeur a en effet amplement discuté de toutes les violations (possibles) et s'est défendu contre la plainte et les accusations. Dans ses conclusions - en résumé -, le défendeur a en effet soutenu avoir pris toutes les mesures techniques et organisationnelles nécessaires ainsi que les autres mesures de précaution afin d'éviter une violation de la vie privée. Le défendeur considère dès lors avoir agi conformément aux articles **5.1.f, 5.2, 24, 32, 33 et 34 du RGPD**. En outre, le défendeur a reconnu qu'il était question d'une fuite de données. Il a toutefois contesté qu'il s'agissait d'une fuite de données susceptible d'engendrer un risque élevé pour les données à caractère personnel

[3] Décision 17/2020 de la Chambre contentieuse https://www.autoriteprotectiondonnees.be/publications/decision-quant-au-fond-n-17-2020.pdf

et dont notification aurait dû être faite auprès de l'Autorité de protection des données (article 33 du RGPD). Le défendeur invoque une autre raison de ne pas effectuer de notification : dans un cas similaire antérieur de fuite de données où la notification avait bel et bien été faite, l'Autorité de protection des données n'avait pris aucune autre mesure envers le défendeur.[4]

Contenu de l'affaire

15. Le plaignant est client chez le défendeur depuis le 11 juin 2015 et utilise des services de téléphonie mobile (prépayés). Le numéro de téléphone du plaignant a été attribué pour une durée de quatre jours, à savoir du 15 au 19 septembre 2019 inclus, à un tiers et à cette occasion, la carte SIM du plaignant a été désactivée.

16. Au cours de cette procédure, la Chambre Contentieuse s'est efforcée de comprendre le déroulement des événements ayant mené à l'attribution du numéro de téléphone du plaignant à un tiers. Il ressort clairement de la présente décision que les tenants et aboutissants du déroulement concret des événements ne peuvent pas être entièrement clarifiés. D'après le défendeur, le tiers s'est rendu le 11 septembre 2019 dans l'un des magasins du défendeur afin de faire convertir l'abonnement prépayé du plaignant en abonnement postpayé (comprenant un smartphone payé après 24 mois d'abonnement). Le défendeur indique qu'à cette occasion, tant le numéro de téléphone que le numéro de carte SIM du plaignant ont été donnés par le tiers. À partir du 11 septembre, l'abonnement du plaignant a dès lors été modifié de prépayé à postpayé. Le tiers a certes communiqué ses propres données d'identité, suite à quoi celles-ci ont été associées à l'abonnement postpayé, de sorte que tous les coûts à compter de ce moment ont été facturés au nom du tiers. Le 11 septembre, le tiers ne disposait toutefois pas encore d'une carte SIM liée au numéro de GSM du plaignant avec pour effet que le plaignant pouvait encore lui-même continuer à bénéficier des services de l'abonnement. Selon le défendeur, quatre jours plus tard, le 15 septembre, le tiers s'est à nouveau rendu dans un magasin Y et a demandé une nouvelle carte SIM liée au même numéro de GSM. À ce moment-là, il a donc obtenu accès au numéro de GSM du plaignant et la carte SIM de ce dernier a été clôturée. À compter de ce moment-là, le plaignant n'avait plus de connexion au réseau.

17. Dans sa plainte, le plaignant explique avoir eu plusieurs contacts téléphoniques avec le défendeur et s'être rendu dans les magasins du défendeur afin de pouvoir à nouveau disposer de son numéro de téléphone. Ce n'est que le 19 septembre que le plaignant a pu à nouveau disposer de son numéro de téléphone.

[4] Voir à ce propos ci-après le point [37].

18. Lors de l'audition, à la demande de la Chambre Contentieuse, le défendeur a donné des explications sur la procédure standard qui est suivie dans des cas comparables à celui-là. Le défendeur affirme - comme déjà indiqué précédemment dans les conclusions - qu'en principe seul l'utilisateur d'un numéro de téléphonie mobile devrait pouvoir connaître le numéro de la carte SIM qui y est liée. C'est la raison pour laquelle le numéro de carte SIM est utilisé pour vérifier que le demandeur est bien l'utilisateur réel du numéro de téléphone qui est donné. Le vendeur aurait dès lors dû demander au tiers en magasin et recevoir de sa part à la fois le numéro de téléphone et le numéro de carte SIM. Selon le défendeur, la migration a alors été effectuée et le tiers a donc donné à cette occasion ses propres données d'identité. D'après le défendeur, les données d'identification du tiers ont été contrôlées en comparant les données de la carte d'identité avec les nom, adresse et domicile renseignés du tiers. Selon le défendeur, ces données d'identité n'ont toutefois pas été comparées avec les données d'identité du client prépayé à qui le numéro de carte SIM et le numéro de GSM avaient été attribués en premier, à savoir le plaignant. Selon le défendeur, ce contrôle n'a pas eu lieu car en vertu de la loi relative aux communications électroniques[5] et du rapport au Roi de l'arrêté royal portant exécution de cette loi, l'utilisation de données d'identité pour des applications commerciale n'est pas autorisée.[6]

19. Le défendeur considère incompréhensible que le tiers ait pu trouver le numéro de carte SIM. D'après le défendeur, le numéro de carte SIM peut uniquement être retrouvé via les systèmes du défendeur où il est enregistré ou si celui-ci est communiqué par le plaignant lui-même. Pour obtenir le numéro de téléphone ainsi que le numéro de carte SIM, le tiers aurait dû - selon le défendeur - bénéficier de la collaboration du plaignant ou de celle d'un collaborateur Y.

20. Pendant l'audition, le défendeur a déclaré que l'introduction d'un numéro de carte SIM par le collaborateur d'un magasin Y est un champ obligatoire ("mandatory") pour effectuer une migration de prépayé à postpayé. Selon le défendeur, le collaborateur doit dès lors demander les données pour ce champ au client et le compléter effectivement pour pouvoir conclure le contrat pour l'abonnement postpayé. D'après le défendeur, un collaborateur d'un magasin Y ne peut pas non plus effectuer de requêtes vers des banques de données de cartes prépayées afin d'obtenir le numéro de carte SIM à l'aide du numéro de GSM. Selon le défendeur, le collaborateur ne pouvait avoir obtenu le numéro de la carte SIM - si le tiers ne lui avait pas donné lui-même - qu'en téléphonant à d'autres collaborateurs Y pour le demander. Pour le défendeur, la probabilité qu'un collaborateur ait aidé le tiers est toutefois faible, notamment parce que le collaborateur n'en aurait

[5] Article 127 juncto l'article 126, § 2, 7° de la loi *relative aux communications électroniques* du 13 juin 2005, entrée en vigueur le 30 juin 2005.
[6] Rapport au Roi de l'arrêté royal du 27 novembre 2016 *relatif à l'identification de l'utilisateur final de services de communications électroniques publics mobiles fournis sur la base d'une carte prépayée,MB* du 7 décembre 2016.

obtenu aucune commission. En outre, le défendeur affirme que dans les jours et les heures proches de la demande de migration, les données du plaignant n'ont fait l'objet d'aucune consultation.

21. Partant de la déclaration du défendeur que les collaborateurs des magasins doivent obligatoirement demander le numéro de carte SIM pour effectuer une migration de préapayé à postpayé et qu'il n'y a aucune possibilité pour le collaborateur de consulter le numéro de carte SIM dans la banque de données à partir du numéro de GSM, la question reste de savoir comment le tiers a pu se procureur la combinaison numéro de GSM - numéro de carte SIM.

22. À la question posée par la Chambre Contentieuse lors de l'audition de savoir s'il a pu s'agir d'un problème de confidentialité de données au niveau d'Y ou dans ses systèmes - par exemple via un accès non autorisé au portail clients en ligne, ayant permis de se procurer le numéro de carte SIM - le défendeur a répondu par la négative. Selon le défendeur, aucun numéro de carte SIM n'est mentionné sur le portail clients d'Y (tant via le navigateur Internet que via l'application mobile). Le défendeur fait en outre savoir lors de l'audition qu'il n'a reçu aucune notification d'autres clients concernant d'éventuels cas d'accès non autorisé à leur numéro de carte SIM.

23. Selon le défendeur, un autre scénario est que le tiers a commis une fraude avec une intention malveillante en obtenant d'une manière ou d'une autre la combinaison du numéro de téléphone et du numéro de la carte SIM du plaignant La Chambre Contentieuse constate toutefois que le tiers a bien renseigné ses propres nom, adresse et domicile, de sorte qu'à partir du 11 septembre, toutes les factures ont abouti chez lui (et entre le 11 et le 15 septembre, le plaignant a même en principe pu utiliser les services d'Y aux frais du tiers). Cela rend la fraude dans le chef du tiers moins plausible. Pendant l'audition, le défendeur avance que le tiers a certes communiqué ses propres données à caractère personnel au défendeur, mais que cela n'empêche pas qu'il puisse toujours être question d'un cas de fraude. D'après le défendeur, le tiers a en effet reçu un téléphone mobile lors de la conclusion de l'abonnement postpayé. Le principe à cet égard est qu'après avoir payé les frais d'abonnement pendant deux ans, l'appareil serait entièrement remboursé. D'après le défendeur, le tiers n'a jamais payé les factures portées en compte pour l'abonnement postpayé. Le défendeur déclare avoir entamé une procédure contre le tiers pour non-paiement des factures. La Chambre Contentieuse ne comprend toutefois pas, dans ce scénario, pourquoi il était nécessaire que le tiers reprenne le numéro de téléphone du plaignant. Dans ce cas, le smartphone pouvait aussi être obtenu simplement en demandant un abonnement postpayé avec un nouveau numéro de GSM.
24. La Chambre Contentieuse estime cette hypothèse de fraude dans le but d'obtenir un smartphone par la reprise du numéro de GSM du plaignent comme étant en l'occurrence assez improbable, d'autant plus que le tiers a communiqué ses propres données à caractère personnel et a conclu

un contrat pour l'abonnement mobile, avec pour effet qu'à partir du 11 septembre, les frais lui étaient aussi facturés.

25. Le défendeur a indiqué tant dans ses conclusions que lors de l'audition qu'il n'était pas possible de comparer l'identité du tiers et celle du titulaire du numéro lié à l'abonnement prépayé. Pour le justifier, le défendeur se réfère aux interdictions imposées par l'article 127 de la loi relatives aux communications électroniques et à l'arrêté royal qui l'exécute[7]. L'arrêté d'exécution contient des modalités relatives à l'identification des utilisateurs finaux de cartes prépayées (prepaid)[8]. D'après le défendeur, la loi et les arrêtés prescrivent que les données d'identification ne peuvent pas être utilisées à des fins commerciales. Le défendeur indique notamment que : *"En raison de l'application stricte de la législation ci-dessus, en cas de demande de migration d'un abonnement prépayé vers un abonnement postpayé, les collaborateurs des points de vente du défendeur peuvent uniquement vérifier le numéro de téléphone et le numéro de carte SIM."*.

26. La partie du préambule de l'arrêté royal citée par le défendeur est formulée en ces termes : *"Par conséquent, les opérateurs et les fournisseurs visés à l'article 126, § 1er, alinéa 1er, ne peuvent pas utiliser à titre commercial les données d'identification collectées en vertu de l'article 127 de la LCE, qui sont conservées en vertu de l'article 126 de la LCE ...".* La Chambre Contentieuse fait remarquer que l'article en question se poursuit toutefois comme suit : *"mais ils peuvent collecter et conserver à titre commercial des données d'identification d'utilisateurs de cartes prépayées conformément à l'article 122 (applicable si une facture est envoyée) ou la législation générale sur la protection de la vie privée."*

27. Pendant l'audition, le défendeur, interrogé sur l'article 127 précité de la LCE, lu conjointement avec l'arrêté royal d'exécution et le rapport au Roi de cet arrêté, a déclaré que la disposition a suscité des discussions chez tous les opérateurs télécom, notamment concernant la question de savoir si l'article devait être lu au sens strict ou pas. Le défendeur interprète l'article de loi au sens strict. Vu qu'il s'agirait en l'espèce de la vente d'abonnements, le défendeur considère cela comme une finalité commerciale.

28. Pour la Chambre Contentieuse, la position du défendeur selon laquelle la réalisation d'un contrôle d'identité (donc en l'occurrence la comparaison des données d'identité du plaignant avec celles du tiers) dans le cadre du passage d'un abonnement prépayé à un abonnement postpayé ne pouvait pas avoir lieu en raison de l'interdiction légale d'utilisation à titre commercial n'est pas correcte.

---

[7] Loi *relative aux communications électroniques* du 13 juin 2005, entrée en vigueur le 30 juin 2005 et arrêté royal d'exécution
[8] Arrêté royal du 27 novembre 2016 *relatif à l'identification de l'utilisateur final de services de communications électroniques publics mobiles fournis sur la base d'une carte prépayée,MB* du 7 décembre 2016.

29. La Chambre Contentieuse se demande s'il est effectivement question ici d'une finalité commerciale, vu que l'utilisation des données d'identité d'un client prepaid aurait en l'occurrence seulement eu pour but de prévenir un abus par une personne qui se présente peut-être indûment dans un magasin Y comme étant l'utilisateur du numéro de téléphone, lié à une carte prépayée. La finalité est donc d'empêcher la reprise indue d'un numéro de téléphone d'un client prepaid par un tiers, qui permettrait à ce dernier d'obtenir également accès aux communications GSM du client et peut-être aussi à d'autres services liés au numéro de téléphone (voir ci-après) avec donc un accès à ses données à caractère personnel. Le défendeur aurait dès lors dû comparer de manière univoque (et donc pas uniquement sur la base d'un numéro de carte SIM qui est tout sauf un authentifiant fort) les données du tiers avec les données du plaignant dont il avait connaissance. Il s'agit en effet ici d'une finalité légitime, à savoir la détection d'une fraude potentielle avec des numéros de téléphone pouvant avoir d'énormes conséquences pour les personnes concernées.

30. À cet égard, la Chambre Contentieuse attire également l'attention sur le rapport au Roi de l'arrêté royal d'exécution[9]. De ce rapport, on peut déduire ce qui suit : Le but du législateur à cet égard n'était pas d'imposer une interdiction générale du contrôle d'identité mais de le soumettre à une réglementation stricte afin de pouvoir garantir un bon niveau de protection des données à caractère personnel. La Chambre Contentieuse estime qu'en n'effectuant aucun contrôle, le défendeur a ignoré la volonté du législateur, à savoir offrir un bon niveau de protection des données à caractère personnel aux personnes concernées. Dans un cas tel que celui-ci, le traitement - limité - de données à caractère personnel en vue de contrôler l'identité vise précisément à éviter l'utilisation abusive de données à caractère personnel.

31. La Chambre Contentieuse estime qu'en l'occurrence, le défendeur aurait pu simplement vérifier si les données sur la carte d'identité du tiers (après vérification de la photo sur la carte d'identité) correspondaient aux données connues du titulaire du numéro de téléphone de la carte prépayée. Le défendeur avait en effet à disposition la carte d'identité du tiers mais a omis de comparer les données à caractère personnel avec celles du titulaire du numéro de GSM, en l'occurrence le plaignant. Une vérification aurait rapidement démontré qu'il s'agissait de deux personnes différentes. Le défendeur a négligé de procéder à cette vérification peu contraignante, alors qu'en tant qu'opérateur télécoms, le défendeur aurait précisément dû avoir conscience des conséquences énormes qu'une telle négligence pouvait entraîner. La Chambre Contentieuse estime cette négligence comme étant disproportionnée.

[9] Rapport au Roi de l'arrêté royal du 27 novembre 2016 *relatif à l'identification de l'utilisateur final de services de communications électroniques publics mobiles fournis sur la base d'une carte prépayée,MB* du 7 décembre 2016.

32. Le défendeur a joint à ses conclusions en réponse un document intitulé *"Méthode de travail Sécurité"*. Ce document interne destiné aux collaborateurs définit la manière dont les données personnelles des clients doivent être traitées et fournit des conseils sur la manière de garantir la confidentialité des données au sein de l'organisation du défendeur.

33. À divers endroits de cette *méthode de travail*, il est indiqué qu'une vérification d'identité complète (nom, prénom, numéro de téléphone, s'il y en a un, numéro de client, adresse, montant de la dernière facture ainsi que l'endroit où et la date à laquelle l'activation est demandée) est requise pour *"Toute demande relative à une modification du contrat, telle que : changement de plan tarifaire, changement d'adresse, P2P, PPP, activation ou désactivation d'un service, demande de copie de facture et demande d'informations confidentielles"* [traduction libre réalisée par le service de traduction de l'APD en l'absence de traduction officielle].

34. En l'espèce, le tiers qui a disposé (ultérieurement) du numéro de téléphone du plaignant a demandé la conversion de sa carte prépayée en un abonnement postpayé. Il a dès lors demandé l'activation d'un nouveau service. Cela signifie que, selon sa propre méthode de travail, le défendeur aurait dû demander des informations supplémentaires dans le but d'établir l'identité de la personne en question. La Chambre Contentieuse considère qu'en omettant d'établir l'identité du tiers avec certitude, le défendeur a fait preuve de négligence blâmable.

35. Le défendeur affirme que la violation a eu des conséquences très limitées pour le plaignant. Selon le défendeur, le tiers n'a pas pu accéder aux profils du plaignant sur différentes plate-formes telles que WhatsApp et Paypal car ces plate-formes utilisent la vérification en deux étapes afin de pouvoir se connecter à leurs profils. D'après le défendeur, le tiers n'avait en outre pas accès à toutes les communications passées du plaignant. Selon le défendeur, il n'est dès lors aucunement question de violation de la vie privée du plaignant. Il est seulement question d'inconvénients pratiques que le plaignant aurait subis.

36. La Chambre Contentieuse relève à cet égard que - contrairement à ce qu'a affirmé le défendeur - pour utiliser par exemple l'application WhatsApp, il suffit en principe que quelqu'un dispose du numéro de téléphone. La vérification en deux étapes qu'il convient de suivre, d'après le défendeur, doit être explicitement activée via les paramètres de WhatsApp et n'est pas configurée par défaut. Le paramétrage de sécurité par défaut est donc que seul le numéro de téléphone suffit pour reprendre l'utilisation de l'application WhatsApp. L'utilisateur introduit le numéro de téléphone via lequel il souhaite utiliser la communication via l'application, et un SMS est ensuite envoyé à ce numéro. Après introduction du code repris dans le SMS, il est directement possible de communiquer via WhatsApp. Si la vérification en deux étapes n'a pas été activée, un accès au numéro de téléphonie mobile auquel le code de vérification a été envoyé suffit.

37. En disposant d'un numéro de téléphone, il existe en outre un risque considérable de pouvoir accéder à différentes sortes de données à caractère personnel. Diverses instances - telles que par exemple des hôpitaux - envoient des rappels de rendez-vous par l'envoi de SMS. En outre, le fait de disposer d'un numéro de téléphone ouvre grand la porte à la fraude et à l'escroquerie (par exemple parce qu'il est possible de mener des conversations ou d'envoyer des messages au nom de la partie lésée). La Chambre Contentieuse n'est donc pas d'accord avec l'affirmation du défendeur selon laquelle il ne serait aucunement question de violation de la vie privée.

38. La Cour de Justice a souligné l'importance des données de télécommunications dans son arrêté "Digital Rights Ireland" du 8 avril 2014 en ces termes : *"Ces données, prises dans leur ensemble, sont susceptibles de permettre de tirer des conclusions très précises concernant la vie privée des personnes dont les données ont été conservées, telles que les habitudes de la vie quotidienne, les lieux de séjour permanents ou temporaires, les déplacements journaliers ou autres, les activités exercées, les relations sociales de ces personnes et les milieux sociaux fréquentés par celles-ci."*[10]. Malgré qu'en l'espèce, le tiers n'ait probablement pas pu disposer de toutes les données citées dans l'arrêt, la Chambre Contentieuse estime que du fait d'avoir disposé du numéro de téléphone du plaignant, il est question d'un risque significatif de violation des droits de ce dernier en matière de respect de la vie privée.

39. L'article 33, paragraphe 1 du RGPD dispose ce qui suit : *"En cas de violation de données à caractère personnel, le responsable du traitement en notifie la violation en question à l'autorité de contrôle compétente conformément à l'article 55, dans les meilleurs délais et, si possible, 72 heures au plus tard après en avoir pris connaissance, à moins que la violation en question ne soit pas susceptible d'engendrer un risque pour les droits et libertés des personnes physiques. Lorsque la notification à l'autorité de contrôle n'a pas lieu dans les 72 heures, elle est accompagnée des motifs du retard."*

40. Le défendeur déclare dans ses conclusions qu'il n'existait pas d'obligation de notifier la fuite de données à l'Autorité de protection des données. La raison en est selon lui que la fuite de données ne touchait qu'une seule personne concernée, qu'elle était de très courte durée et qu'il estimait qu'elle n'impliquait pas de données sensibles. Par rapport à ce qui précède, la Chambre Contentieuse attire l'attention sur le point évoqué ci-dessus, à savoir que l'on peut considérer plausible que, par exemple, des SMS contenant des données personnelles particulières aient été reçus.

---

[10] Cour de Justice UE, Digital Rights Ireland et Seitlinger e.a, affaires jointes C-293/12 et C-594/12, ECLI:EU:C:2014:238 , pt. 27.

41. Pour évaluer si une violation est susceptible de constituer un risque élevé pour les droits et libertés des personnes physiques, il convient selon les Directives du Groupe 29 de tenir compte de la réponse à la question de savoir si la violation peut entraîner des dommages physiques, matériels ou immatériels pour les personnes dont les données font l'objet de la violation. Des exemples de tels dommages sont la discrimination, le vol ou l'usurpation d'identité, la perte financière et une atteinte à la réputation[11]. En attribuant le numéro de téléphone du plaignant à un tiers, on expose le plaignant au risque que des actes frauduleux soient effectués en son nom, en utilisant son numéro de téléphone. Le risque existe également - contrairement à ce que semble affirmer le défendeur - que des données sensibles (telles que des données de santé) tombent entre les mains de tiers. Le défendeur affirme qu'il n'existait pas d'obligation de notification dans son chef, notamment car il s'agissait d'une violation de données d'une seule personne. La Chambre Contentieuse souligne qu'une violation, même si elle ne touche qu'une seule personne, peut toutefois avoir de graves conséquences, en fonction de la nature des données à caractère personnel et du contexte dans lequel elles ont été compromises. Ici encore, il convient d'examiner la probabilité et la gravité des conséquences[12]. Selon la Chambre Contentieuse, il s'agit en outre ici d'un risque de nature structurelle auquel tous les utilisateurs de cartes prépayées peuvent potentiellement être exposés. On ne peut pas exclure qu'il existe d'autres cas dont la Chambre Contentieuse n'est pas au courant.

42. Le défendeur soumet à l'Autorité de protection des données une notification antérieure datée du 11 mars 2019 concernant une fuite de données similaire[13]. Il y indique qu'une autre raison de ne pas notifier la fuite dans ce cas était la suivante : *"L'Autorité de protection des données n'a pas donné suite à ce dossier, ce qui montre l'importance limitée que l'Autorité de protection des données accorde à ces (petites) fuites de données. Ceci a confirmé la présomption du défendeur selon laquelle il n'y avait pas d'obligation de notification dans le cas présent."* [Traduction libre effectuée par le service traduction de l'Autorité de protection des données, en l'absence de traduction officielle]. La Chambre Contentieuse attire l'attention à cet égard sur la responsabilité du défendeur qui découle de l'article 5.2 et de l'article 24 du RGPD, en vertu de laquelle il lui incombe de démontrer qu'il se conforme aussi à l'article 5.1.f) du RGPD, à savoir : *"garantir une sécurité appropriée des données à caractère personnel traitées, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle ("intégrité et confidentialité"), à l'aide de mesures techniques ou organisationnelles."* L'affirmation selon laquelle une notification précédente n'a pas été traitée par l'Autorité de protection des données n'enlève rien à la responsabilité.

---

[11] Lignes directrices concernant la notification d'une violation de données à caractère personnel en vertu du Règlement 2016/679, Groupe 29, p. 26.

[12] Idem, p. 30.

[13] En tant que pièce 5 dans ses conclusions.

43. La Chambre Contentieuse rappelle une fois de plus qu'en vertu de l'article 5, paragraphe 2, de l'article 24 et de l'article 32 du RGPD, la responsabilité implique que le responsable du traitement prenne les mesures techniques et organisationnelles nécessaires afin de veiller à ce 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 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.

44. Dans son Avis relatif au "principe de responsabilité", le Groupe 29 informe que deux aspects sont importants pour l'interprétation de ce principe :

    (i) " *"la nécessité pour le responsable du traitement des données de prendre des mesures appropriées et efficaces pour mettre en œuvre les principes de protection des données ; et*

    (ii) *la nécessité de démontrer, sur demande, que des mesures appropriées et efficaces ont été prises. En conséquence, le responsable devrait fournir des preuves de l'exécution du point (i) ci-dessus"*[14]*.*

45. La Chambre Contentieuse estime que dans le cas présent, le défendeur n'a pas réussi à démontrer que des mesures proactives ont été prises pour garantir le respect du RGPD. Les collaborateurs du défendeur ont tout d'abord omis d'effectuer une vérification entre l'identité du tiers et celle du plaignant et Y a ensuite négligé de notifier la fuite de données à l'Autorité de protection des données. Le défendeur n'a fourni aucune pièce prouvant que l'obligation de documentation qui lui incombait a été respectée. Le seul document fourni par le défendeur concernant une fuite de données était une notification d'une autre fuite de données par le défendeur à l'Autorité de protection des données datant de 2019. Il ressort des pièces du dossier, de ce qui a été dit à l'audition et de l'absence d'introduction par le défendeur de toute documentation relative à la fuite de données que le défendeur ne respecte pas non plus l'obligation de l'article 33, paragraphe 5 du RGPD, qui prévoit que :

    "Le responsable du traitement documente toute violation de données à caractère personnel, en indiquant les faits concernant la violation des données à caractère personnel, ses effets

[14] Avis 3/2010 sur le principe de la responsabilité adopté le 13 juillet 2010 par le Groupe 29, pp. 10-14, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp173_fr.pdf.

et les mesures prises pour y remédier. La documentation ainsi constituée permet à l'autorité de contrôle de vérifier le respect du présent article."

46. La Chambre Contentieuse a déjà souligné précédemment dans sa décision 2020/22 que : *"la responsabilité appliquée aux fuites de données implique qu'un responsable du traitement a non seulement la responsabilité de notifier les fuites de données le cas échéant à l'autorité de contrôle et aux personnes concernées, conformément aux articles 33 et 34 du RGPD, mais aussi qu'il doit pouvoir démontrer à tout moment qu'il a pris les mesures nécessaires afin de pouvoir respecter cette obligation"*[15]*.* La Chambre Contentieuse estime que dans le cas présent, cela ne peut pas être démontré.

47. Dans une liste non exhaustive de mesures que les responsables du traitement peuvent prendre pour satisfaire à la responsabilité, le Groupe 29 renvoie, entre autres, aux mesures suivantes à prendre : la mise en œuvre et la surveillance des procédures de contrôle pour s'assurer que toutes les mesures n'existent pas seulement sur le papier mais sont également exécutées et fonctionnent dans la pratique, l'établissement de procédures internes, l'élaboration d'une politique écrite et contraignante en matière de protection des données, le développement de procédures internes pour la gestion et la notification efficaces de violations de la sécurité.

48. La Chambre Contentieuse attire également l'attention sur un formulaire joint aux conclusions qui mentionnait une fuite de données similaire, à savoir le numéro de téléphone d'un client qui avait changé d'opérateur. Ce numéro de téléphone avait été considéré à tort comme libre et attribué à un autre client. Dans le formulaire, à la question *"Quel est le degré ou le niveau de gravité de la fuite de données pour les personnes concernées lors de l'analyse des risques pour les droits et libertés des personnes concernées ?"*, il est à noter que le défendeur a répondu que la fuite de données était "critique". Selon la Chambre Contentieuse, cela montre clairement que le défendeur comprend aussi la gravité d'une telle fuite de données.

49. La Chambre Contentieuse constate dès lors une violation de l'article 33, paragraphes 1er et 5, et de l'article 34, paragraphes 1er et 2 du RGPD. La Chambre Contentieuse souligne qu'il existe dans le chef du responsable du traitement une obligation de documenter chaque fuite de données, qu'elle comporte des risques ou non, afin de pouvoir fournir des informations à l'APD. Le traitement de données à caractère personnel est en effet une activité centrale du défendeur. Les données à caractère personnel peuvent en outre présenter un degré de sensibilité élevé pour les personnes concernées, notamment parce qu'elles permettent une observation régulière et systématique[16]. Le plaignant aurait aussi dû être informé de la fuite de données en vertu de l'article 34.1. Bien que

[15] Décision 22/2020 du 8 mai 2020 de la Chambre Contentieuse , p. 12.

[16] Décision 18/2020 du 28 avril 2020 de la Chambre Contentieuse.

le plaignant était déjà au courant de la fuite de données en appelant son propre numéro, le défendeur aurait également dû lui communiquer cette fuite sans délai, conformément aux exigences de l'article 34, paragraphe 2. L'article précité prévoit en effet que la notification doit comporter la nature de la violation, les coordonnées du délégué à la protection des données ou d'un autre point de contact auprès duquel des informations supplémentaires peuvent être obtenues et les mesures que le responsable du traitement a proposées ou prises.

50. La Chambre Contentieuse déduit raisonnablement de l'omission du défendeur d'introduire dans la procédure une communication au sens de l'article 34 du RGPD qu'une telle communication n'a pas été faite au plaignant. Le défendeur a dès lors négligé, après qu'il ait été lui-même au courant, d'informer le plaignant au moyen d'une communication conforme à l'article 34, paragraphe 2, de l'attribution du numéro de téléphone de ce dernier à un tiers. La Chambre Contentieuse rejette l'affirmation du défendeur selon laquelle une communication à la personne concernée n'était pas nécessaire dans ce cas au motif qu'il n'était pas question d'un risque élevé. La Chambre Contentieuse se réfère dans ce cadre à l'exemple suivant dans les *"Guidelines on Examples regarding Data Breach Notification"* récemment publiées par l'EDPB, dans lequel le centre de contact d'une société de télécommunications reçoit un appel d'une personne qui prétend être un client et demande de changer son adresse e-mail afin que les factures soient désormais envoyées à cette nouvelle adresse e-mail. L'appelant fournit les données personnelles correctes du client, après quoi les factures sont envoyées à la nouvelle adresse électronique. Lorsque le véritable client appelle la société pour demander pourquoi il ne reçoit plus de factures, la société se rend compte que les factures sont envoyées à quelqu'un d'autre.

51. Par rapport à l'exemple ci-dessus, l'EDPB envisage ce qui suit :

"This case serves as an example on the importance of prior measures. The breach, from a risk aspect, presents a high level of risk, as billing data can give information about the data subject's private life (e.g.habits, contacts)and could lead to material damage (e.g. stalking, risk to physical integrity). The personal data obtained during this attack can also be used in order to facilitate account takeover in this organisation or exploit further authentication measures in other organisations. Considering these risks, the "appropriate" authentication measure should meet a high bar, depending on what personal data can be processed as a result of authentication.

As a result, both a notification to the SA and a communication to the data subject are needed from the controller. The prior client validation process is clearly to be refined in light of this case. The methods used for authentication were not sufficient. The malicious party was able to pretend to be the intended user by the use of publicly available information and information that they otherwise had access to. The use of this type of static knowledge-based authentication (where the

answer does not change, and where the information is not "secret" such as would be the case with a password) is not recommended."[17]

52. La notification de violations doit être considérée comme une manière d'améliorer le respect des règles en matière de protection des données à caractère personnel. Lorsqu'une violation relative à des données à caractère personnel se produit ou s'est produite, elle peut occasionner des dommages matériels ou immatériels à des personnes physiques ou tout autre dommage économique, physique ou social pour la personne concernée. Par conséquent, dès que le responsable du traitement a connaissance d'une violation de données à caractère personnel présentant un risque pour les droits et libertés des personnes concernées, il doit, sans retard injustifié et, si possible, dans les 72 heures, notifier la violation à l'autorité de contrôle. Cela permet à l'autorité de contrôle d'exercer correctement ses missions et ses pouvoirs tels qu'ils sont définis dans le RGPD.

4. Violations du RGPD

53. La Chambre Contentieuse estime que les violations des dispositions suivantes par le défendeur sont avérées :
    a. **articles 5.1.f, 5.2, 24 et 32 du RGPD**, vu que le défendeur n'a pas pris suffisamment de mesures de précaution pour prévenir la fuite de données ;
    b. **les articles 33.1, 33.5 et 34.1 du RGPD**, vu que le défendeur n'a pas notifié la fuite de données à l'APD et à la personne concernée.

54. La Chambre Contentieuse estime approprié d'infliger une amende administrative d'un montant de 25.000 euros (article 83, deuxième paragraphe du RGPD ; article 100, § 1er, 13° de la LCA et article 101 de la LCA).

55. Compte tenu de l'article 83 du RGPD et de la[18] jurisprudence de la Cour des marchés, la Chambre Contentieuse motive l'imposition d'une sanction administrative de manière concrète :

    a) La gravité de la violation : la Chambre Contentieuse constate que la fuite de données est notamment due à de la négligence de la part du défendeur. Le défendeur a en outre omis de notifier la fuite à l'Autorité de protection des données, et tant dans ses conclusions que lors de l'audition, il a affirmé que vu qu'il n'était pas question en l'espèce d'une opération

[17] EDPB *Guideline on Examples regarding Data Breach Notification,* 01/2021, p. 30 *Soulignement par la Chambre Contentieuse.*
[18] Cour d'appel de Bruxelles (section Cour des Marchés), *X c. APD,* Arrêt 2020/1471 du 19 février 2020.

susceptible d'engendrer un risque élevé pour les droits et les devoirs du plaignant, il n'y aurait pas d'obligation de notification dans son chef. Comme il s'agit en l'occurrence d'une fuite de données de télécommunications à partir desquelles des données précises relatives à la vie privée d'une personne peuvent être obtenues, ainsi que du risque potentiel de voir commettre des actes frauduleux au nom de cette personne, il est question d'une infraction grave.

b) La durée de la violation : la violation a duré quatre jours, ce qui constitue une durée considérable à la lumière du risque potentiel pointé ci-avant.

c) La Chambre Contentieuse considère que l'amende à infliger et l'injonction de mettre le traitement en conformité sont suffisamment dissuasives pour prévenir de telles violations à l'avenir.

56. La Chambre Contentieuse attire l'attention sur le fait que les autres critères de l'article 83.2 du RGPD ne sont pas, dans ce cas, de nature à conduire à une autre amende administrative que celle définie par la Chambre Contentieuse dans le cadre de la présente décision.

57. Dans sa réaction à l'intention d'infliger une amende, le défendeur s'est opposé au montant de l'amende envisagée. D'après la Chambre Contentieuse, il est toutefois apparu dans ce dossier qu'il a été question de négligence envers la protection des données à caractère personnel de la personne concernée. Le traitement de données à caractère personnel représente en effet une activité principale du défendeur, d'où l'importance fondamentale de traiter les données à caractère personnel conformément au RGPD.

58. Les faits, les circonstances et les violations constatées justifient donc une amende qui réponde à la nécessité d'avoir un effet suffisamment dissuasif, le défendeur étant sanctionné avec une sévérité suffisante afin que les pratiques impliquant de telles infractions ne se reproduisent pas.

59. 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.

60. Dans sa réaction à l'amende envisagée, le défendeur a demandé de ne pas publier la décision, pas même sous une forme anonymisée. La Chambre Contentieuse refuse cette demande en se référant à la note qu'elle a publiée sur le site Internet de l'APD concernant la publication de décisions, dans laquelle on peut lire ce qui suit : *La Chambre Contentieuse part du principe que*

toutes ses décisions, sauf exceptions, font l'objet d'une publication sur son site web, dans un objectif général de transparence, mais également de visibilité et de responsabilité."[19].

PAR CES MOTIFS,

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

- d'ordonner au défendeur, conformément à l'article 100, § 1er, 9° de la LCA, de mettre le traitement en conformité avec les articles 5.1.f, 5.2, 24 et 32 du RGPD, en mettant en particulier la politique vis-à-vis de l'identification et de la vérification des clients prépayés en conformité avec le RGPD. À cet effet, la Chambre Contentieuse accorde au défendeur un délai de trois mois et attend du défendeur qu'il lui fasse un rapport dans le même délai concernant la mise en conformité du traitement avec les dispositions susmentionnées.

- en vertu de l'article 83 du RGPD et des articles 100, 13° et 101 de la LCA, d'infliger au défendeur une amende administrative de **25.000 euros** pour violation des article 5.1.f, 5.2, 24, 32, 33.1 et 5, et 34.1 du RGPD.

En vertu de l'article 108, § 1er de la LCA, un recours peut être introduit contre cette décision dans un délai de trente jours, à compter de la notification à la Cour des marchés, avec l'Autorité de protection des données comme défendeur.

(sé.) Hielke Hijmans
Président de la Chambre Contentieuse

19 https://www.autoriteprotectiondonnees.be/publications/politique-de-publication-des-decisions-de-la-chambre-contentieuse.pdf