Autorité de protection des données
Gegevensbeschermingsautoriteit

Chambre Contentieuse

Décision quant au fond 101/2022 du 3 juin 2022

Le recours contre cette décision a été rejeté par l'arrêt 2022/AR/889 de la Cour des marchés du 22 février 2023

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 Dirk Van Der Kelen et Yves Poullet ;

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, représenté par Me B. Bruyndonckx et Me L. Kuyken, tous deux ayant leurs bureaux Avenue du port 86c b113, 1000 Bruxelles, ci-après "le défendeur"

I. Faits et procédure

Déroulement de la procédure

1. Le 22 janvier 2021, la Chambre Contentieuse a pris la décision 05/2021 à l'égard du défendeur, par le biais de laquelle une amende de 25.000 EUR lui a été imposée suite à une violation des articles 5.1.f, 5.2, 24, 32, 33.1 et 5 et 34.1 du RGPD.

- Le 19 février 2021, le défendeur a interjeté appel de la décision 05/2021 de la Chambre Contentieuse.

- Le 20 mai 2021, la Chambre Contentieuse a retiré sa décision du 22 janvier 2021 par le biais de la décision de retrait 61/2021 et a ainsi décidé de reconsidérer l'affaire au moyen d'une nouvelle procédure quant au fond.

- Le 30 juin 2021, la Cour des marchés a rendu un arrêt dans le cadre du recours introduit par Y.

- Le 23 septembre 2021, la Chambre Contentieuse a envoyé le nouveau calendrier des conclusions aux parties afin de permettre le lancement d'une nouvelle procédure quant au fond.

- Le 2 novembre 2021, la Chambre Contentieuse a reçu les conclusions en réponse de la part du défendeur.

- Le 25 avril 2022, le défendeur est entendu par la Chambre Contentieuse, conformément à l'article 53 du règlement d'ordre intérieur de l'Autorité de protection des données.

2. La présente décision est basée sur une nouvelle procédure quant au fond. La Chambre Contentieuse a en effet retiré sa première décision 05/2021 suite à la plainte dans le dossier en question et a décidé d'entamer une nouvelle procédure quant au fond. La présente décision est dès lors prise sur la base de la plainte, des conclusions introduites et d'autres pièces pertinentes de l'affaire.

La plainte et la première décision subséquente de la Chambre Contentieuse

3. 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 concernait 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 avait été désactivée et le tiers aurait donc

pu prendre 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.

4. 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. Le 27 mai 2020, le défendeur a introduit des conclusions en réponse. Le 9 novembre 2020, le défendeur est entendu par la Chambre Contentieuse, conformément à l'article 53 du règlement d'ordre intérieur. Le 19 novembre 2020, le procès-verbal de l'audition est soumis aux parties. 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.

5. Ensuite, la Chambre Contentieuse a pris la décision 05/2021 le 22 janvier 2021, par le biais de laquelle une amende de 25.000 EUR a été infligée au défendeur suite à une violation des articles 5.1.f, 5.2, 24, 32, 33.1 et 5 et 34.1 du RGPD.

6. Le 19 février 2021, Y a introduit un recours auprès de la Cour des marchés contre la décision de la Chambre Contentieuse du 22 janvier 2021. Y déclarait dans le recours que lors de sa prise de décision, la Chambre Contentieuse avait méconnu les droits de la défense et violé les principes de bonne administration. Le défendeur affirmait notamment que le principe de proportionnalité avait été violé car la Chambre Contentieuse n'avait pas demandé d'enquête au Service d'Inspection. D'après le défendeur, la Chambre Contentieuse avait également violé le principe de motivation et le principe d'équité en prenant une décision disproportionnée aux yeux du défendeur et en imposant une amende trop élevée. Le défendeur estimait qu'en ne lui donnant pas l'occasion de présenter son point de vue sur la base d'une accusation concrète, les droits de la défense avaient été violés. Selon le défendeur, la Chambre Contentieuse avait conclu à tort à l'existence de violations des articles 5.1.f, 5.2, 24, 32, 33.1 et 5, ainsi que 34.1 du RGPD.

7. Dans l'attente de l'appel, la décision susmentionnée a été retirée par la Chambre Contentieuse par la décision de retrait 61/2021. Dans cette décision, la Chambre Contentieuse a considéré ce qui suit :

"Considérant que dans ses arrêts 2020/AR/813 du 18 novembre 2020 et 2021/AR/1159 du 24 février 2021, la Cour des marchés a souligné l'importance d'informer les parties concernées préalablement à l'examen du dossier à propos des allégations et/ou violations exactes dont elles pourraient se rendre coupables ; Considérant que lors du recours devant la Cour des marchés contre la décision quant au fond 5/2021 du 22 janvier 2021, la SA Y a fait valoir qu'il n'avait pas

été suffisamment informé des allégations et/ou violations exactes dans la procédure précédant cette décision.

A décidé :
. de retirer par la présente décision la décision quant au fond 5/2021 du 22 janvier 2021 rendue contre la SA Y.
. de rouvrir la procédure devant la Chambre Contentieuse et, conformément à l'article 98 de la loi APD, d'inviter les parties à introduire de nouvelles conclusions." [Traduction libre effectuée par le Secrétariat Général de l'Autorité de protection des données en l'absence de traduction officielle]

8. La décision de retrait de la Chambre Contentieuse n'a fait l'objet d'aucun recours par le défendeur. Lors de l'examen du recours contre la première décision de la Chambre Contentieuse, le défendeur a cependant affirmé que la Cour des marchés "*devrait à nouveau examiner l'affaire quant au fond en utilisant sa compétence de pleine juridiction et substituer sa propre décision à celle de la Chambre Contentieuse.*" [Tous les passages cités du dossier ont été traduits librement par le Secrétariat Général de l'Autorité de protection des données en l'absence de traduction officielle]

9. Le 30 juin 2021, la Cour des marchés a rendu son arrêt. La Cour y a toutefois considéré la demande susmentionnée du défendeur comme suit *:*

"Vu que la décision du 19 mai 2021 indique qu'il a été décidé "de rouvrir la procédure devant la Chambre Contentieuse et d'inviter les parties, conformément aux dispositions de l'article 98 de la LCA, à présenter de nouvelles conclusions" et qu'aucun recours n'a été introduit contre cette décision, Y a accepté que la Cour des marchés ne puisse pas prendre de décision propre dans cette affaire hic et nunc et que la Chambre Contentieuse devait d'abord avoir la possibilité de rouvrir la procédure." [Traduction libre effectuée par le Secrétariat Général de l'Autorité de protection des données en l'absence de traduction officielle][1]

10. Par ce qui précède, la Cour des marchés a donc confirmé que la décision de la Chambre Contentieuse ayant fait l'objet d'un recours par le défendeur n'existait plus dans les échanges juridiques et, en vertu de la décision de retrait, était réputée n'avoir jamais existé. La requête du défendeur selon laquelle la Cour des marchés devrait prendre sa propre décision en se substituant à la Chambre Contentieuse en vertu de sa compétence de pleine juridiction a donc été déclarée infondée par la Cour des marchés. Le recours est sans objet.

11. La Cour des marchés a également relevé que le retrait de la décision ne pouvait pas être considéré en soi comme une preuve que la Chambre Contentieuse a pris une décision *erronée* ou *illégale*. Selon la Cour des marchés, il n'est pas non plus question d'un quelconque

[1] Considérant 7.5 de l'arrêt de la Cour des marchés

comportement fautif dans le chef de la Chambre Contentieuse. Au contraire, la Cour des marchés considère que le retrait témoigne du respect des principes de l'État de droit par la Chambre Contentieuse.

Nouvelle procédure quant au fond

12. Le 23 septembre 2021, la Chambre Contentieuse a envoyé un nouveau calendrier de conclusions aux parties. Dans ce courrier, la Chambre Contentieuse a également énuméré les faits reprochés au défendeur comme suit : "Il est reproché au défendeur :

1. de ne pas avoir vérifié, ou d'avoir vérifié de manière insuffisante ou incorrecte, si la tierce personne qui a demandé, dans le magasin du défendeur, la migration de sa carte SIM de prépayé à postpayé en déclarant être titulaire du numéro de téléphone était bien cette personne. Suite à ce qui précède, son[2] numéro a été attribué à la tierce personne et celle-ci a pu disposer du numéro de téléphone et prendre connaissance des appels téléphoniques du plaignant, ce qui implique qu'il était question d'une fuite de données. Il est dès lors reproché au défendeur de ne pas avoir pris les mesures techniques et organisationnelles nécessaires pour empêcher une violation de la vie privée du plaignant (articles 5.1.f, 5.2, 24 et 32 du RGPD)

2. de ne pas avoir notifié la fuite de données résultant de la pratique décrite au point 1 à l'Autorité de protection des données ni à la personne concernée, en l'occurrence le plaignant (articles 33.1, 33.5 et 34.1 du RGPD)".

13. La Chambre Contentieuse a en outre formulé les questions suivantes, afin d'obtenir davantage de clarté :

"1. Le défendeur a-t-il pris toutes les mesures techniques et organisationnelles nécessaires conformément aux articles 5.1.f, 24 et 32 du RGPD et offert un niveau de sécurité adéquat afin d'empêcher l'attribution - prétendue - du numéro de téléphone du plaignant à un tiers et, dans l'affirmative, peut-il le prouver ?

2. Le défendeur peut-il démontrer qu'il a pris des mesures proactives conformément à l'article 5.2 du RGPD pour assurer le respect des règles du RGPD, y compris les mesures mentionnées ci-dessus au point 1 ?

3. Le défendeur considère-t-il qu'il y a eu une fuite de données et a-t-il ensuite respecté l'obligation de notifier cette fuite de données à l'Autorité de protection des données conformément à l'article 33.1 du RGPD, a-t-il documenté ces violations conformément à

[2] On vise le numéro de téléphone du plaignant.

l'article 33.5 du RGPD et en a-t-il également informé la personne concernée conformément à l'article 34.1 du RGPD ?

14. Les délais pour déposer des conclusions ont été fixés :

- au 2 novembre 2021 comme date limite pour la réception des conclusions en réponse du défendeur ;
- au 23 novembre 2021 comme date limite pour la réception des conclusions en réplique du plaignant ;
- au 14 décembre 2021 comme date limite pour la réception des conclusions en réplique du défendeur.

15. Le 2 novembre 2021, la Chambre Contentieuse a reçu les conclusions en réponse du défendeur, mettant en avant les moyens suivants :

- Le défendeur a pris toutes les mesures techniques et organisationnelles nécessaires conformément aux articles 5.1.f), 24 et 32 du RGPD et a offert un niveau de sécurité adéquat ;
- Le défendeur a pris des mesures proactives conformément à l'article 5.2 du RGPD afin de garantir le respect des prescriptions du RGPD, dont les mesures techniques et organisationnelles ;
- Le défendeur a agi conformément aux articles 33 et 34 du RGPD ;
- Selon le défendeur, la Chambre Contentieuse devra siéger dans une composition totalement différente compte tenu de l'arrêt de la Cour des marchés rendu en ce sens. Si la composition de la Chambre Contentieuse dans cette procédure n'était pas totalement différente de celle de la Chambre Contentieuse qui s'est prononcée le 22 janvier 2021, le défendeur considérerait la composition comme étant irrégulière, de même que la procédure.

16. Le 25 avril 2022, les parties sont entendues par la Chambre Contentieuse.

17. Le 9 mai 2022, le procès-verbal de l'audition est transmis aux parties.

18. Le 17 mai 2022, la Chambre Contentieuse reçoit du défendeur des réactions au procès-verbal. Tout d'abord, le défendeur affirme que le président, Hielke Hijmans, aurait "admis" lors de l'audition que la décision de la Cour des marchés stipulant que si une affaire est traitée un seconde fois par la Chambre Contentieuse, comme en l'occurrence, la Chambre Contentieuse doit siéger dans une composition totalement différente, n'aurait pas été respectée par la Chambre Contentieuse. Le défendeur estime en outre que le procès-verbal ne restitue pas suffisamment ce que les membres auraient déclaré pendant l'audition. Aucune précision n'est donnée quant à ce qui manquerait exactement.

19. Le 16 mai 2022, le formulaire de sanction a été envoyé au défendeur.

20. Le 31 mai 2022, la Chambre Contentieuse reçoit la réaction du défendeur au formulaire de sanction.

Contenu de l'affaire

21. 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.

22. 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 cette 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 2019, 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 2019, 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 2019, le tiers s'est à nouveau rendu dans un magasin d'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.

23. 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 2019 que le plaignant a pu à nouveau disposer de son numéro de téléphone.

II. Motivation

2.1 À propos de la composition de la Chambre Contentieuse

24. Tant dans ses conclusions que lors de l'audition, le défendeur a clairement exprimé des réserves quant à la composition de la Chambre Contentieuse. Le défendeur a souligné lors de l'audition que la composition de la Chambre Contentieuse n'était pas entièrement constituée d'autres personnes physiques et a noté que les deux membres avaient été remplacés alors que le président continuait à siéger pendant cette procédure. En outre, le défendeur a déclaré dans sa réaction au procès-verbal que le président aurait reconnu ne pas respecter la décision de la Cour des marchés. L'affirmation qui précède est inexacte. La Chambre Contentieuse exposera ci-après, de manière motivée, les raisons pour lesquelles cette composition de la Chambre Contentieuse a été choisie pour traiter ce dossier.

25. La Cour des marchés a en effet décidé dans son arrêt du 30 juin 2021 que la Chambre Contentieuse "*serait composée dans son intégralité de personnes physiques autres qui celles qui faisaient partie de la Chambre lorsque la décision actuellement contestée a été prise.*" Le défendeur affirme dès lors que la procédure est illégale si la Chambre Contentieuse n'est pas composée de trois personnes autres que celles qui faisaient partie de la Chambre Contentieuse lorsque la première décision a été prise.

26. La Cour a également jugé que : "*Bien que les membres de la Chambre Contentieuse ne soient pas des juges, il convient que cet organe respecte les règles de base de la bonne administration, y compris au moins l'apparence d'impartialité*".

27. La Chambre Contentieuse souligne qu'en l'espèce, il n'est pas question d'une quelconque illégalité constatée par la Cour des marchés dans les actes de la Chambre Contentieuse. Il n'est absolument pas question d'un arrêt mettant en cause l'impartialité de la Chambre Contentieuse. L'inverse est vrai. La Cambre Contentieuse a choisi de retirer sa première décision avec la motivation suivante :

> *"Considérant que dans ses arrêts 2020/AR/813 du 18 novembre 2020 et 2021/AR/1159 du 24 février 2021, la Cour des marchés a souligné l'importance d'informer les parties concernées préalablement à l'examen du dossier à propos des allégations et/ou infractions exactes dont elles pourraient se rendre coupables ; Considérant que lors du recours devant la Cour des marchés contre la décision quant au fond 5/2021 du 22 janvier 2021, Y a fait valoir qu'il n'avait pas été suffisamment informé des allégations et/ou infractions exactes dans la procédure précédant cette décision."*

28. Rien n'indique que la Chambre Contentieuse - telle qu'elle a été constituée à l'origine - aurait été partiale et ne pourrait pas (en partie ou même entièrement dans la même composition) statuer à nouveau sur l'affaire.

29. La décision de retrait de la Chambre Contentieuse n'a en outre fait l'objet d'aucun recours par le défendeur. Le défendeur a demandé à la Cour des marchés de substituer sa propre décision à celle de la Chambre Contentieuse et de statuer sur le fond du recours qu'elle a introduit contre la première décision et qui a été retirée par la Chambre Contentieuse dans l'attente du recours. La Cour des marchés a rejeté la demande du défendeur en considérant que la décision attaquée était réputée n'avoir jamais existé dans les échanges juridiques du fait de la décision de retrait prise par la Chambre Contentieuse. Le recours était dès lors devenu sans objet. La Cour des marchés a relevé à cet égard que le retrait de la décision ne pouvait pas être considéré en soi comme une preuve que la Chambre Contentieuse a pris une décision *erronée* ou *illégale*. La Cour des marchés considère que le retrait témoigne du respect des principes de l'État de droit par la Chambre Contentieuse.

30. Dans un arrêt du 7 août 2018, la Cour des marchés s'est prononcée sur la question de principe de savoir si, après l'annulation d'une décision en raison d'un vice de procédure, une affaire doit être réexaminée par un organe composé différemment, ou si cet organe peut prendre une nouvelle décision avec la même composition. Il s'agissait d'une décision de l'Autorité belge de la Concurrence (ABC). Dans cet arrêt, la Cour des marchés a décidé qu'une composition différente était nécessaire dans ce cas, car l'article IV.30 du *Code de droit économique* (CDE) rendait l'article 828 du *Code judiciaire* applicable à l'ABC. L'article 828 du *Code judiciaire* reprend les causes de récusation pour les juges. Dans cet arrêt, l'élément crucial était que la Cour des marchés avait estimé que l'article 828 du *Code judiciaire* pouvait être appliqué à des personnes autres que les juges faisant partie du pouvoir judiciaire *uniquement* si la loi le prévoit explicitement. Vu que la LCA ne contient aucune disposition qui déclare l'article 828 du *Code judiciaire* applicable aux membres de la Chambre Contentieuse, ces derniers ne peuvent pas être récusés sur la base de cette disposition s'ils ont déjà eu connaissance du même litige.

31. La Chambre Contentieuse s'efforce de respecter le principe d'impartialité en tant que principe général de bonne administration et met tout en œuvre pour y parvenir afin d'assurer un procès équitable aux parties. Ce principe garantit en effet à la fois l'impartialité personnelle des membres de la Chambre Contentieuse qui prennent une décision et l'impartialité structurelle de la Chambre Contentieuse en ce qui concerne son organisation, le déroulement de la procédure et la prise de ses décisions.[3]

32. D'après la jurisprudence constante du Conseil d'État, le principe d'impartialité s'applique toutefois uniquement aux organes de l'administration active "*pour autant que cela soit*

[3] Voir, par analogie, avis du Conseil d'État du 26 février 2015, n° 230.338, *Députation du conseil provincial d'Anvers*, considérant 10.

compatible avec la nature propre, en particulier la structure de l'autorité publique".[4] Plus précisément, l'application du principe ne peut pas conduire à ce que la prise d'une décision régulière devienne impossible, notamment parce que ce principe empêcherait l'intervention de l'organe administratif compétent.[5] Dans la mesure où l'application du principe aboutirait, par exemple, à ce qu'un organe ne puisse plus exercer ses compétences légales, l'application de ce principe sera écartée.

33. La Chambre Contentieuse se compose d'un président et de six membres dont trois francophones et trois néerlandophones.[6] Ces membres ont tous leur propre domaine d'expertise. Lors de l'examen d'un dossier devant la Chambre Contentieuse, les membres sont dès lors impliqués sur la base de la langue qu'ils parlent et de leur expertise. Comme indiqué ci-avant, le principe d'impartialité s'applique dans la mesure où il est compatible avec la nature et la structure de l'autorité publique. Lors du premier examen de la plainte contre le défendeur, les deux membres néerlandophones Frank De Smet et Jelle Stassijns siégeaient avec le président. Cela signifie qu'il ne reste plus qu'1 membre néerlandophone. Pour cette seule raison, il n'est déjà pas possible que la Chambre Contentieuse siège dans une composition totalement différente, car cela n'est tout simplement pas compatible avec la nature et la structure de la Chambre Contentieuse et entraverait sérieusement la continuité de la Chambre Contentieuse. Vu que la connaissance de la langue dans laquelle une plainte est traitée devant la Chambre Contentieuse est indispensable pour un traitement efficace, les membres chargés d'examiner un dossier déterminé sont tout d'abord désignés par le président - conformément à l'article 33 de la LCA et à l'article 43 du Règlement d'ordre intérieur - sur la base de la langue parlée et, bien entendu, de l'expertise dans le domaine concerné. En ce qui concerne le rôle linguistique, le point de départ est que - en plus du président qui satisfait aux exigences linguistiques pour toutes les langues nationales - au moins un membre appartient au rôle linguistique de la langue de la procédure (et l'autre membre a une connaissance factuelle suffisante de la langue).

34. La Chambre Contentieuse rappelle que d'après la doctrine, le principe de bonne administration et d'impartialité est moins important et moins strict que le principe de bonne administration de la justice qui vaut pour le juge. Dans tous les cas, l'administré a en effet la possibilité d'introduire un recours auprès d'un juge qui répond aux exigences de l'article 6.1 de la CEDH.[7]

35. La Cour de Justice a estimé que même la composition d'une formation *de jugement* ne doit pas être totalement modifiée après renvoi.[8] D'après la Cour "*la circonstance qu'un même juge siège*

---

[4] Voir par ex. avis du Conseil d'État du 3 octobre 2014, n° 228.633, ASBL *Unsolicited Artists* ; 10 décembre 2020, n° 249.191, considérant 25.

[6] Article 40, § 1er de la loi portant création de l'Autorité de protection des données.

[7] Avis du Conseil d'État du 23 avril 2009, n° 192.590, *Crauwels*, considérant 3.2.4. Voir aussi I. OPDEBEEK et S. DE SOMER, *Algemeen bestuursrecht. Grondslagen en beginselen*, Antwerpen, Intersentia, 2017, 384-385.

[8] CJUE, C-341/06 P et C-342/06 P, *Chronopost et La Poste/UFEX e.a.*, 1er juillet 2008, EU:C:2008:375, §§ 51-60.

dans deux formations de jugement [du Tribunal] ayant eu successivement *à connaître de la même affaire ne saurait, par elle-même, en dehors de tout autre élément objectif, faire naître un doute sur l'impartialité du Tribunal.*" "*[...] Il n'apparaît pas que le renvoi de l'affaire devant une formation de jugement composée d'une manière totalement distincte de celle qui a eu à connaître du premier examen de l'affaire doive et puisse, dans le cadre du droit communautaire, être considéré comme une obligation à caractère général.*"

36. À l'appui de leur jugement, les juridictions de l'Union se réfèrent à la jurisprudence de la Cour européenne des droits de l'homme (CEDH), qui a déjà jugé à plusieurs reprises qu' "*il ne saurait être posé en principe général découlant du devoir d'impartialité qu'une juridiction annulant une décision administrative ou judiciaire a l'obligation de renvoyer l'affaire à une autre autorité juridictionnelle ou à un organe autrement constitué de cette autorité*". Ainsi, concernant un collège disciplinaire, la CEDH a jugé que l'on ne pouvait voir un motif de suspicion légitime de partialité dans la circonstance qu'après annulation en cassation de la première décision à laquelle ils avaient pris part, trois des sept membres de ce collège aient à nouveau dû se prononcer sur la même affaire.[9]

37. Bien qu'il n'y ait aucune illégalité établie dans les actes de la Chambre Contentieuse ou de doutes sur son impartialité, le président de la Chambre Contentieuse a décidé de satisfaire à la demande du défendeur dans la mesure du possible et a désigné, dans le cas présent, deux autres membres - à savoir Monsieur Dirk Van Der Kelen et Monsieur Yves Poullet - pour siéger lors du traitement de la présente procédure quant au fond. Le président continuera dès lors à siéger lui-même, étant donné que d'un point de vue pratique, il est irréalisable pour la Chambre Contentieuse de siéger dans une composition totalement différente, compte tenu du nombre de membres dans les deux rôles linguistiques.

2.2 Conclusions et analyse de la Chambre Contentieuse

Première conclusion : le défendeur a pris toutes les mesures techniques et organisationnelles nécessaires conformément aux articles 5.1.f), 24 et 32 du RGPD et a ainsi offert un niveau de sécurité adéquat.

38. Le défendeur avance comme première conclusion qu'il a pris toutes les mesures techniques et organisationnelles nécessaires conformément aux articles 5.1.f), 24 et 32 du RGPD et qu'il a ainsi offert un niveau de sécurité adéquat. Selon le défendeur, plusieurs éléments permettent de démontrer qu'un niveau de sécurité adéquat a été offert. Tout d'abord, le défendeur applique des règles internes concernant les mesures techniques et organisationnelles qui doivent être respectées au sein de l'organisation. Le défendeur prend toujours les mesures techniques et

[9] CEDH, *Diennet c. France*, 26 septembre 1995, § 38.

organisationnelles appropriées pour sécuriser les données à caractère personnel de ses abonnés. Les mesures prises sont évaluées chaque année et adaptées au besoin. En outre, l'Institut belge des services postaux et des télécommunications (IBPT) effectue un audit annuel des mesures techniques et organisationnelles au sein de l'organisation. En raison de sa confidentialité, le document ne peut pas être présenté dans le cadre de la présente procédure, selon le défendeur. En outre, le défendeur a une obligation de secret des communications qui découle de l'article 124 de la loi *relative aux communications électroniques* (LCE).

39. Les documents Y *Belgium overzicht van Technische en Organisatorische maatregelen et Group Security Standard*[10] sont de nouveaux documents dont la Chambre Contentieuse n'a pas pu prendre connaissance plus tôt. Le document *Group Security Standard* contient les mesures de sécurité obligatoires devant être prises par le *Y Group*. Il concerne un point de référence partagé du *Y Group* et décrit les exigences de sécurité minimales devant obligatoirement être mises en œuvre par chaque entité. Le document contient des principes généraux en matière de sécurité, de sécurité de l'information et de sécurité physique. Le document Y *Belgium overzicht van Technische en Organisatorische maatregelen* contient également des principes généraux.

Concernant la vérification de l'identité

40. 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. Le défendeur souligne toutefois que la procédure interne a été modifiée suite à la décision de la Chambre Contentieuse du 22 janvier 2021 ordonnant notamment la mise en conformité du traitement avec les articles 24 et 32 du RGPD. Depuis lors, le défendeur applique donc comme procédure standard la vérification de l'identité lors de la conversion de cartes prépayées en cartes postpayées. Dans ce contexte, un accès a été donné aux collaborateurs des magasins afin d'effectuer ce contrôle. Selon le défendeur, la raison pour laquelle aucun contrôle n'a été effectué plus tôt est entièrement liée aux interdictions imposées par l'article 127 de la loi *relative aux communications électroniques* et par l'arrêté royal portant exécution de cette loi[11]. L'arrêté d'exécution contient des modalités relatives à l'identification des utilisateurs finaux de cartes prépayées (prepaid).[12] 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*

[10] Ces documents ont été introduits dans la procédure avec les conclusions.

[11] Loi *relative aux communications électroniques* du 13 juin 2005, entrée en vigueur le 30 juin 2005 et arrêté royal d'exécution.

[12] 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.

points de vente du défendeur peuvent uniquement vérifier le numéro de téléphone et le numéro de carte SIM."

41. 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 attire l'attention sur le fait que l'article précité se termine toutefois en ces termes : "*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*."

42. Pendant l'audition, le défendeur a déclaré à propos de l'article 127 précité de la LCE, lu conjointement avec l'arrêté royal d'exécution et le rapport au Roi de cet arrêté, 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.

43. 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.

44. La Chambre Contentieuse estime, contrairement au défendeur, qu'il ne s'agit pas ici d'une finalité commerciale. Tout d'abord, le but de l'utilisation des données d'identité d'un client prépayé est en l'espèce uniquement d'empêcher l'utilisation abusive du numéro de téléphone par d'éventuelles personnes non autorisées, comme dans le cas présent. La finalité est donc d'empêcher la reprise indue d'un numéro de téléphone d'un client prépayé 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. 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 identifiant fort) les données du tiers avec les données du plaignant dont il avait connaissance. En résumé, il s'agit 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.

45. À cet égard, la Chambre Contentieuse attire également l'attention sur le rapport au Roi de l'arrêté royal d'exécution.[13] Dans ce rapport, on peut lire 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.*" 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.

46. Le défendeur déclare également dans ses conclusions :

> *"Si la Chambre Contentieuse estime toutefois que le concluant était néanmoins tenu de comparer l'identité avec celle du titulaire du numéro de téléphone, elle interprète avec particulièrement de souplesse la réglementation et les directives auxquelles le responsable du traitement est soumis. Rien n'indique que telle était l'intention du législateur, on ne pouvait donc pas s'attendre à ce que le concluant adopte une telle position."*

47. Contrairement à l'affirmation du défendeur, la Chambre Contentieuse considère que l'article 18, § 1er de l'arrêté royal portant exécution de l'article 127, § 1er de la LCE et expliquant cette disposition est très clair et ne laisse aucune place au doute quant à son interprétation et à son application. L'article dispose notamment ce qui suit :

> *"L'entreprise concernée s'assure, en mettant en place des mesures techniques et opérationnelles, que la personne qui demande l'extension du produit est effectivement la personne identifiée pour ce produit."*

48. Le commentaire des articles de l'arrêté royal apporte l'explication suivante à cet article :

> *"Art. 18. L'extension ou la migration de produit. Une personne peut déjà être cliente d'une entreprise concernée pour un autre produit (par exemple un abonnement à la téléphonie mobile) et avoir été identifiée par l'entreprise concernée pour ce produit. Elle peut alors décider d'acheter en complément une carte prépayée (l'extension de produit) ou de passer du premier produit vers une carte prépayée (la migration de produit). L'entreprise concernée peut alors établir un lien entre la carte prépayée et le produit déjà acheté par l'utilisateur final. L'entreprise concernée s'assure, en mettant en place des mesures techniques et opérationnelles, que la personne qui demande l'extension du produit est effectivement la personne identifiée pour ce produit. Ceci peut être par exemple fait par la présentation d'un document d'identité ou à l'aide du numéro d'identifiant et d'un mot de passe. La personne qui est le titulaire du produit auquel la carte prépayée est associée doit être la même personne que celle qui demande l'activation de*

[13] 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.

la carte prépayée. Cette méthode ne peut donc pas être utilisée si un enfant demande l'activation de la carte prépayée en se référant à un autre produit souscrit par un parent. "[14] (soulignement propre).

49. Il ressort donc clairement et de manière univoque de ce qui précède que l'entreprise concernée (en l'occurrence le défendeur) a elle-même une obligation légale, en cas de migration de produit, de s'assurer de l'identité de la personne qui demande la migration. L'objectif de ce qui précède est d'obtenir la certitude qu'il s'agit bien de la personne identifiée pour ce produit. Il ressort en outre de l'Exposé des motifs que la vérification peut uniquement avoir lieu après présentation d'un document d'identité ou à l'aide d'un numéro d'identifiant et d'un mot de passe.

50. Compte tenu de la formulation claire et sans équivoque du législateur dans la réglementation susmentionnée, qui, selon la Chambre Contentieuse, ne laisse place à aucune autre interprétation, une vérification de l'identité aurait dû avoir lieu. La Chambre Contentieuse considère que le défendeur aurait bel et bien dû procéder au contrôle de l'identité de la personne qui demandait la migration de la carte SIM. Le législateur prescrit en effet explicitement que ce contrôle doit s'effectuer sur la base de la carte d'identité ou d'un numéro d'identifiant et d'un mot de passe.

51. Le défendeur ne pouvait donc pas se contenter de demander le numéro de la carte SIM et le numéro de téléphone. 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.

52. 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. Le défendeur a ainsi délibérément omis de se conformer à une obligation légale, à savoir celle prévue à l'article 18, § 1er de l'arrêté royal portant exécution de la loi *relative aux communications électroniques*. La Chambre Contentieuse en conclut qu'il n'était pas seulement question d'un manquement imputable mais aussi d'une violation de l'article 18, § 1er de l'arrêté royal qui prescrit clairement qu'un contrôle doit avoir lieu en cas de migration de produit.

53. Tout au long de la procédure, le défendeur a fait valoir que la migration de produit devait être considérée comme une finalité commerciale et que, par conséquent, il était interdit de procéder à une vérification d'identité. Il ressort toutefois de l'article 18, § 1er de l'arrêté royal que le législateur ne qualifie pas la migration de produit de finalité commerciale et prescrit précisément

[14] 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. (soulignement propre de la Chambre Contentieuse)

qu'une vérification de l'identité doit avoir lieu. Dès lors, l'argument du défendeur ne tient pas la route.

54. Dans sa première décision, la Chambre Contentieuse a notamment considéré que le défendeur devait mettre le traitement en conformité avec les articles 5.1.f), 5.2, 24 et 32 du RGPD. Le défendeur a exécuté cette injonction en adoptant une procédure supplémentaire pour vérifier l'identité du client en cas de migration de produit. À cet égard, le défendeur indique toutefois dans ses conclusions que cela a été fait au risque que le défendeur soit réprimandé par l'IBPT ou par un tribunal par rapport à l'utilisation des données d'identification à des fins commerciales, ce qui serait expressément interdit par l'article 126 de la LCE.

55. La Chambre Contentieuse conclut que selon la législation en vigueur, une migration de produit ne peut pas être considérée comme une finalité commerciale. Elle constate donc que le manquement aux articles 5.1.f), 5.2, 24 et 32 du RGPD perdure.

Deuxième conclusion : le défendeur a pris des mesures proactives conformément à l'article 5.2 du RGPD afin de garantir le respect des prescriptions du RGPD, dont les mesures techniques et organisationnelles.

56. Dans sa deuxième conclusion, le défendeur affirme avoir bel et bien pris des mesures proactives afin de garantir le respect des prescriptions du RGPD, dont les mesures techniques et organisationnelles. Le défendeur a joint à ses conclusions en réponse un document intitulé "*Werkmethode Veiligheid*". Ce document interne destiné aux collaborateurs définit la manière dont les données à caractère personnel 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.

57. 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, date de naissance, numéro de carte d'identité, 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'Autorité de protection des données en l'absence de traduction officielle]

58. 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. En omettant d'établir l'identité du tiers avec certitude, le défendeur a fait preuve de négligence répréhensible.

59. Le défendeur a en outre introduit les documents *Y Belgium overzicht van Technische en Organisatorische maatgregelen* et *Group Security Standard* dans la procédure (voir le point 39 ci-avant).

60. Selon le défendeur, ces documents permettent également de déduire que le défendeur se soucie de prendre à tout moment les mesures techniques et organisationnelles appropriées pour sécuriser les données à caractère personnel de ses abonnés. Les mesures prises sont également évaluées et, au besoin, adaptées chaque année par ses soins. Les deux documents comportent des exigences minimales générales de sécurité à mettre en œuvre. Sur la base de ces documents, la Chambre Contentieuse ne peut toutefois pas parvenir à une autre conclusion qu'en l'occurrence, le défendeur a manqué à ses devoirs en ne mettant pas en œuvre de manière adéquate les mesures techniques et organisationnelles.

61. 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 plateformes telles que WhatsApp et Paypal car ces plateformes utiliseraient la vérification en deux étapes afin de pouvoir se connecter à ses 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.

62. 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 est envoyé suffit.

63. 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 - procèdent à 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 serait 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.

64. 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 : *"Prises dans leur ensemble, lesdites données peuvent 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.*[15] " 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 était question d'un risque significatif de violation des droits de ce dernier en matière de respect de la vie privée.

65. Le défendeur affirme dans les conclusions qu'en principe, seul l'utilisateur d'un numéro de téléphone 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'identification. 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*[16] et du rapport au Roi de l'arrêté royal portant exécution de cette loi, l'utilisation de données d'identité[17] pour des applications commerciales n'est pas autorisée, comme expliqué aux points 42 e.s. ci-dessus.

66. 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 d'Y. D'après

---

[15] 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 , r.o. 27.

[16] 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.

[17] 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.

le défendeur, la combinaison entre la carte SIM et le numéro de téléphone est unique, de sorte que la méthode consistant à utiliser la combinaison du numéro de téléphone et du numéro de la carte SIM est appropriée pour vérifier l'identité de l'utilisateur. Si seul le numéro de téléphone était utilisé pour vérifier l'identité de l'utilisateur pour la migration, cela pourrait toutefois, selon le défendeur, indiquer des mesures techniques et organisationnelles défaillantes. Selon le défendeur, la combinaison du numéro de téléphone et du numéro de carte SIM peut être assimilée à la combinaison de l'adresse e-mail et du mot de passe. Dans cette combinaison également, la vérification consiste en un élément public et un élément que seul le propriétaire peut connaître.

67. La Chambre Contentieuse attire l'attention sur la déclaration du défendeur selon laquelle :

- les collaborateurs devaient obligatoirement demander le numéro de carte SIM au client et saisir ce numéro afin d'exécuter une migration de prépayé à postpayé ;
- il n'existait à l'époque aucune possibilité pour le collaborateur de rechercher le numéro de carte SIM dans la base de données à l'aide du numéro de GSM.

Dès lors, la question de savoir comment le tiers a obtenu la combinaison du numéro de GSM et du numéro de carte SIM reste entière. Le défendeur n'a en tout cas pas été en mesure de le démontrer face à la Chambre Contentieuse, comme requis par les articles 5.2 et 24 du RGPD.

68. Le défendeur soumet à l'Autorité de protection des données une notification antérieure datée du 11 mars 2019 concernant une fuite de données similaire.[18] 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 concluant selon laquelle il n'y aurait 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 antérieure n'a pas été traitée par l'Autorité de protection des données n'enlève rien à la responsabilité.

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

69. 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.

70. 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*".[19]

71. Compte tenu des considérations ci-dessus, la Chambre Contentieuse estime que le défendeur a commis une **violation des articles 5.1.f), 5.2, 24 et 32 du RGPD** en ne prenant pas de mesures techniques et organisationnelles suffisantes pour garantir que le traitement de données à caractère personnel se déroule conformément à la législation et à la réglementation pertinentes.

Fuite de données

72. 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.*"

[19] 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.

73. 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 à caractère personnel particulières aient été reçus.

74. Pour évaluer si une violation est susceptible de constituer un risque élevé pour les droits et libertés des personnes physiques, il convient selon les Lignes directrices 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.[20] 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.[21] 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.

75. 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 produit 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

[20] Lignes directrices *sur la notification d'une violation de données à caractère personnel en vertu du règlement (UE) 2016/679, wp250rev.01,* Groupe 29, p. 26.

[21] Idem, p. 30.

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

76. 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*[22]". La Chambre Contentieuse estime que dans le cas présent, cela ne peut pas être démontré.

77. 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.

78. 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.

79. La Chambre Contentieuse constate dès lors une violation de l'article 33, paragraphes 1 et 5 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'Autorité de protection des données. Le traitement de données à caractère personnel est en effet une activité centrale du défendeur. Les données à

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

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.[23]

80. Le défendeur joint à ses conclusions un document *Data Breach Assessment*. Ce document renseigne la fuite de données au 15 avril 2020, soit 7 mois après que la fuite de données se soit produite. Dans ce document, on peut notamment lire ce qui suit*:*

"L'incident a permis à un tiers d'accéder au contenu des communications du client à partir d'une carte prépayée pendant 3,25 jours. Le tiers n'avait pas l'intention d'utiliser les données, d'en abuser ou de les diffuser. Les données n'étaient dès lors pas disponibles publiquement sur Internet.
L'impact théorique de la violation est donc très grand, vu qu'il s'agit du contenu des communications, et bien que la probabilité que la violation ait des conséquences pour la personne concernée soit faible, il en résulte un risque global très élevé.

Toutefois, sur la base des informations reçues de la personne concernée, le contenu des communications partagé avec un tiers était probablement limité aux codes d'authentification en deux étapes, et ce pour une période de 3,5 jours. Ces codes d'identification en deux étapes ne peuvent pas être utilisés par la partie tierce qui n'a pas accès aux données de connexion de la personne concernée. Les conséquences pour la personne concernée sont donc limitées et le risque a été ramené à un risque faible." [Traduction libre effectuée par le Secrétariat Général de l'Autorité de protection des données, en l'absence de traduction officielle]

81. Il ressort à nouveau du texte cité ci-dessus que le défendeur était bel et bien conscient du fait qu'en l'espèce, il était question d'un "risque très élevé", vu qu'il s'agissait du contenu de télécommunications. Le risque a été ramené à "faible" après que le défendeur a appris que le contenu partagé était probablement limité à des codes d'authentification en deux étapes. Vu que des tiers ne pouvaient accéder aux données de connexion du plaignant, le niveau a donc été revu à la baisse. Comme la Chambre Contentieuse l'a déjà fait remarquer, ce ne sont pas seulement les applications nécessitant une authentification en deux étapes qui présentaient un risque pour le plaignant, mais ses communications téléphoniques et par SMS étaient également exposées à des risques élevés, notamment de fraude qui aurait pu être commise en son nom. La Chambre Contentieuse considère qu'il était bel et bien question d'un risque élevé.

82. Le défendeur estime qu'il n'était pas obligé d'informer le plaignant de la fuite de données. Le défendeur a dès lors négligé, après qu'il ait été lui-même au courant, d'informer le plaignant

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

au moyen d'une communication, de l'attribution du numéro de téléphone de ce dernier à un tiers. La Chambre Contentieuse estime que dans ce cas particulier, la notification à la personne concernée pouvait ne pas avoir lieu compte tenu des circonstances particulières de cette affaire, où la personne concernée avait déjà connaissance de la fuite de données. La Chambre Contentieuse estime donc qu'**aucune violation de l'article 34 du RGPD ne peut être constatée.**

83. La Chambre Contentieuse cite l'exemple ci-dessous, qui illustre une nouvelle fois l'importance de la communication d'une fuite de données aux personnes concernées et à l'autorité compétente. Il s'agit d'un exemple récemment publié dans les *"Guidelines on Examples regarding Data Breach Notification"* récemment publiées par l'EDPB[24], 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 à caractère personnel correctes du client, après quoi les factures sont envoyées à la nouvelle adresse e-mail. 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.

84. 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."[25]

[24] EDPB *Guideline on Examples regarding Data Breach Notification,* 01/2021, publié sur www.edpb.europa.eu.

[25] EDPB *Guideline on Examples regarding Data Breach Notification,* 01/2021, p. 30 (Soulignement par la Chambre Contentieuse).

Traduction libre : Ce cas illustre l'importance de prendre des mesures préalables. Du point de vue des risques, la violation représente un risque élevé car les données de facturation peuvent fournir des informations sur la vie privée de la personne concernée (par ex. ses habitudes, ses contacts) et peuvent engendrer des dommages matériels (par ex. harcèlement, risque pour l'intégrité physique). Les données à caractère personnel obtenues lors de cette attaque peuvent également être utilisées pour faciliter la prise de contrôle de

85. 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. Dès lors, la Chambre Contentieuse estime qu'il n'est pas question de "notifications excessives et non nécessaires" comme l'affirme le défendeur. Le Groupe 29 affirme en effet à cet égard que :

"Les responsables du traitement devraient garder à l'esprit que la notification à l'autorité de contrôle est obligatoire, à moins que la violation en question ne soit pas susceptible d'engendrer un risque pour les droits et libertés des personnes physiques. En outre, lorsqu'une violation est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, ces dernières doivent également être informées. Le seuil à atteindre est par conséquent plus élevé pour la communication aux personnes concernées que pour la notification à l'autorité de contrôle, et toutes les violations ne devront donc pas être communiquées aux personnes concernées, ce qui les protège de notifications excessives et non nécessaires."[26]

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, en règle générale, 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.

Réaction au formulaire d'amende et droit de la défense

86. Le défendeur a réagi à l'intention d'infliger une amende le 31 mai 2022.

87. Le défendeur y répète que selon lui, la composition de la Chambre Contentieuse est irrégulière, tout comme la procédure, vu que le président a continué à siéger malgré la décision de la Cour des marchés. Selon le défendeur, il n'a pas été prouvé qu'il était question d'une fuite de données

comptes dans cette organisation ou pour exploiter d'autres mesures d'authentification dans d'autres organisations. Compte tenu de ces risques, la mesure d'authentification "appropriée" doit répondre à des exigences et, en fonction de celles-ci, il est possible de déterminer quelles données à caractère personnel peuvent être traitées.

Cela nécessite à la fois une notification à l'autorité de contrôle et une communication à la personne concernée par le responsable du traitement. Le processus de validation préalable des clients doit clairement être affiné à la lumière de ce cas. Les méthodes qui étaient utilisées pour l'authentification n'étaient pas suffisantes. Une personne malintentionnée aurait pu se faire passer pour l'utilisateur visé en utilisant des informations disponibles publiquement ainsi que des informations auxquelles elle avait accès par d'autres moyens. L'utilisation de ce type d'authentification statique basée sur la connaissance (où la réponse ne change pas et où l'information n'est pas "secrète" comme ce serait le cas avec un mot de passe) n'est pas recommandée."

[26] Lignes directrices *sur la notification d'une violation de données à caractère personnel en vertu du règlement (UE) 2016/679*, Groupe 29, WP25 0.rev.01

et la constatation de l'existence d'une fuite de données repose uniquement sur des présomptions. Le plaignant n'a apporté aucune preuve de l'existence d'une fuite de données. Le défendeur estime qu'il a pris suffisamment de mesures techniques et organisationnelles afin de prévenir un incident comme en l'espèce. Le défendeur déclare à plusieurs reprises avoir tenu compte des règles de la Loi *relative aux communications électroniques* (LCE) et indique que la loi précitée interdit le contrôle et la vérification de l'identité dans le cadre de finalités commerciales. D'après le défendeur, la migration d'une carte SIM doit être considérée comme une finalité commerciale. Le défendeur indique que dans une décision précédente de la Chambre Contentieuse, la politique de sécurité qu'il applique avait été qualifiée d'appropriée. Le défendeur répète qu'il n'y avait aucune obligation de notifier la fuite de données à l'Autorité de protection des données, vu qu'elle 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 à caractère personnel sensibles.

88. Le défendeur ne peut se rallier à la conclusion de la Chambre Contentieuse selon laquelle il a été question d'un "*degré disproportionné de négligence*", vu que le défendeur met tout en œuvre pour protéger les données à caractère personnel le mieux possible. En outre, il n'y a pas eu d'intention ou de mauvaise volonté de la part du défendeur. Le défendeur estime que l'amende envisagée de 20.000 EUR n'est pas proportionnée aux violations qui ont été constatées. D'après le défendeur, l'imposition d'une amende contraste fortement avec les décisions antérieures de la Chambre Contentieuse dans lesquelles de tels cas impliquant une seule personne concernée et ayant un impact sociétal limité auraient été classés sans suite. Le défendeur affirme être victime d'une personne malhonnête qui a su obtenir les données à caractère personnel du plaignant. Il n'est pas non plus question de violations antérieures commises par le défendeur. Tout ceci rend l'imposition d'une amende de 20.000 EUR excessive. Le défendeur trouve qu'un avertissement serait plus approprié. Si la Chambre Contentieuse décidait malgré tout d'imposer une amende, le défendeur demande à la Chambre Contentieuse de limiter l'amende à un montant de 5.000 EUR. En ce qui concerne les chiffres annuels, le défendeur indique qu'il y a une légère différence avec les chiffres annuels présentés par la Chambre Contentieuse dans le formulaire de sanction ; le montant correct est 1.3XX.XXX.XXX EUR au lieu de 1.2XX.XXX.XXX EUR.

89. La Chambre Contentieuse estime que tous les arguments avancés par le défendeur dans le formulaire de sanction ont déjà été examinés dans la présente décision et ont été pris en considération pour fixer l'amende administrative conformément à l'article 83.2 du RGPD. La Chambre Contentieuse a en effet expliqué dans la décision que la fuite de données est due à une négligence dans le chef du défendeur. Selon la Chambre Contentieuse, le défendeur aurait dû, tant sur la base de la LCE qu'en vertu de la réglementation interne, vérifier les données d'identification afin de s'assurer que la personne qui se trouvait dans le magasin était aussi effectivement le titulaire du numéro de téléphone. Ce que le défendeur a négligé de faire. Il a en outre négligé d'en adresser une notification à l'Autorité de protection des données. La Chambre

Contentieuse ne partage pas le point de vue du défendeur selon lequel il n'existe aucune preuve que des tiers aient eu connaissance des données à caractère personnel, empêchant ainsi de démontrer l'existence d'une fuite de données. Comme la Chambre Contentieuse l'a indiqué au point 63, il existait une forte probabilité que le tiers ait eu accès aux données à caractère personnel (sensibles) du plaignant ; ce tiers a en effet eu accès au numéro de téléphone pendant quatre jours. Il ne peut donc pas être exclu qu'un accès de ce tiers aux données à caractère personnel du plaignant ait eu lieu.

90. Il s'agit en l'espèce d'un responsable du traitement qui traite quotidiennement des quantités massives de données dont on peut attendre qu'il prenne les mesures techniques et organisationnelles appropriées pour assurer la protection des données à caractère personnel. Compte tenu de ce qui précède, la Chambre Contentieuse estime qu'une amende de 20.000 EUR peut être qualifiée de très limitée par rapport aux violations constatées et au chiffre d'affaires qui ressort des chiffres annuels du défendeur.

91. Enfin, la Chambre Contentieuse attire l'attention sur le fait qu'il n'y a aucune obligation dans son chef, ni sur la base du RGPD ou de la LCA, ni sur la base de la jurisprudence de la Cour des marchés, de soumettre à la contradiction de la partie défenderesse la motivation de la présente décision préalablement à la prise de la décision en question, le formulaire de sanction servant uniquement à offrir la possibilité de s'opposer à l'amende envisagée.

3. Violations du RGPD

92. La Chambre Contentieuse estime que les violations des dispositions suivantes par le défendeur sont avérées :

    a. **les 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 et 33.5 du RGPD,** vu que le défendeur n'a pas notifié la fuite de données à l'Autorité de protection des données**.**

93. La Chambre Contentieuse estime approprié d'infliger une amende administrative d'un montant de 20.000 EUR (article 83, paragraphe 2 du RGPD ; article 100, § 1er, 13° de la LCA et article 101 de la LCA).

94. Compte tenu de l'article 83 du RGPD et de la jurisprudence[27] de la Cour des marchés, la Chambre Contentieuse motive l'imposition d'une amende administrative de *manière concrète* :

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

a.) La gravité de la violation : la Chambre Contentieuse constate que la fuite de données est notamment due à de la négligence dans le chef du défendeur. Le défendeur a en outre omis de notifier la fuite à l'Autorité de protection des données, et il a affirmé que vu qu'il n'était pas question en l'espèce d'une opération 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 violation 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.) L'amende à infliger est suffisamment dissuasive pour prévenir de telles violations à l'avenir. La Chambre Contentieuse répète que dans ce contexte, une amende de 20.000 EUR peut être qualifiée de très limitée par rapport aux violations constatées et au chiffre d'affaires qui ressort des chiffres annuels du défendeur.

95. 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.

96. Par souci d'exhaustivité, la Chambre Contentieuse renvoie également aux lignes directrices sur le calcul des amendes administratives (*Guidelines 04/2022 on the calculation of administrative fines under the GDPR*) publiées par l'EDPB sur son site Internet le 16 mai 2022, pour consultation. Vu que ces lignes directrices ne sont pas encore définitives, la Chambre Contentieuse a décidé de ne pas encore les prendre en considération pour déterminer le montant de l'amende dans la présente procédure.

97. 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 centrale du défendeur, d'où l'importance fondamentale de traiter les données à caractère personnel conformément au RGPD.

98. 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.

99. 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, 13° et 101 de la LCA, d'infliger au défendeur une amende administrative de **20.000 euros** pour violation des article 5.1.f, 5.2, 24, 32, 33.1 et 33.5 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.

(sé.) Hielke Hijmans
Président de la Chambre Contentieuse