



Chambre Contentieuse

Décision quant au fond 62/2024 du 25 avril 2024

Numéro de dossier : DOS-2020-00171

Objet : Sécurité et utilisation du numéro de Registre national dans un système de prise de rendez-vous en ligne

La Chambre Contentieuse de l'Autorité de protection des données, composée de Monsieur Hielke Hijmans, président, et de Messieurs Dirk Van Der Kelen et Jelle Stassijns, membres ;

Vu le Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 *relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE* (Règlement général sur la protection des données, ci-après "RGPD") ;

Vu la loi du 3 décembre 2017 *portant création de l'Autorité de protection des données*, ci-après "LCA" ;

Vu le règlement d'ordre intérieur tel qu'approuvé par la Chambre des représentants le 20 décembre 2018 et publié au *Moniteur belge* le 15 janvier 2019 ;

Vu les pièces du dossier ;

A pris la décision suivante concernant :

La plaignante : Madame X, ci-après "la plaignante" ;

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

I. Faits et procédure

1. Le 10 février 2020, la plaignante introduit une plainte auprès de l'Autorité de protection des données contre le défendeur.
2. L'objet de la plainte concerne l'utilisation du numéro d'identification du Registre national dans le système de prise de rendez-vous en ligne du défendeur et les mesures (de sécurité) techniques et organisationnelles y afférentes.
3. Le 5 mars 2020, la plainte est déclarée recevable par le Service de Première Ligne sur la base des articles 58 et 60 de la LCA et la plainte est transmise à la Chambre Contentieuse en vertu de l'article 62, § 1^{er} de la LCA.
4. Le 26 mars 2020, conformément à l'article 96, § 1^{er} de la LCA, la demande de la Chambre Contentieuse de procéder à une enquête est transmise au Service d'Inspection, de même que la plainte et l'inventaire des pièces.
5. Le 4 mai 2020, l'enquête du Service d'Inspection est clôturée, le rapport est joint au dossier et celui-ci est transmis par l'Inspecteur Général au Président de la Chambre Contentieuse (art. 91, § 1^{er} et § 2 de la LCA).

Le rapport du Service d'Inspection contient les constatations suivantes :

1. Violation de l'article 30.2 du RGPD en raison d'un registre des activités de traitement incomplet et imprécis ;
 2. Violation de l'article 32.1 du RGPD en raison de l'absence de mesures techniques et organisationnelles appropriées, et violation de l'article 32 du RGPD en raison d'une collaboration insuffisante à l'enquête du Service d'Inspection ;
 3. Pas de violation de l'article 28.3 du RGPD suite à la présentation de contrats de sous-traitance par le défendeur ;
 4. Violation de l'article 37.1 du RGPD en raison de l'absence de désignation d'un délégué à la protection des données ;
 5. Traitement du numéro de Registre national par le défendeur pour le compte de ses clients.
6. Le 20 novembre 2020, la Chambre Contentieuse décide, sur la base de l'article 95, § 1^{er}, 1^o et de l'article 98 de la LCA, que le dossier peut être examiné sur le fond et informe les parties concernées par envoi recommandé des dispositions telles qu'énoncées à l'article 95, § 2 et à l'article 98 de la LCA. Elles sont également informées, en vertu de l'article 99 de la LCA, des délais pour transmettre leurs conclusions.

La date limite pour la réception des conclusions en réponse de la plaignante a été fixée au 11 décembre 2020 et celle pour les conclusions en réplique du défendeur au 4 janvier 2021.

7. Le 24 novembre 2020, le défendeur accepte toutes les communications relatives à l'affaire par voie électronique et manifeste son intention de transmettre des conclusions, ce conformément à l'article 98 de la LCA.
8. Le 10 décembre 2020, la Chambre Contentieuse reçoit les conclusions en réponse de la plaignante. Celle-ci déclare reconnaître les violations telles que constatées par le Service d'Inspection. La plaignante fait également valoir que l'utilisation du numéro de Registre national comme identifiant unique semble pour l'instant illicite et demande qu'il soit démontré que le défendeur relève d'une exception telle que visée à l'article 8 de la loi du 8 août 1983 *organisant un registre national des personnes physiques*. La plaignante se réfère en outre à l'article 13 de la loi susmentionnée en ce qui concerne les conséquences d'une utilisation illicite du numéro de Registre national. À cet égard, la plaignante déclare partir du principe que le défendeur demandera ou a déjà demandé entretemps une autorisation d'utiliser le numéro de Registre national.
9. Le 4 janvier 2021, la Chambre Contentieuse reçoit les conclusions en réplique du défendeur qui déclare en substance effectuer le traitement de données pour le compte des responsables du traitement qui ont répondu à son offre SaaS¹, raison pour laquelle il affirme intervenir en tant que sous-traitant. Le défendeur répond à chaque constatation du Service d'Inspection et soumet des arguments et des pièces pour réfuter les violations constatées par le Service d'Inspection. Par ailleurs, le défendeur objecte également que l'intérêt de la plaignante n'a pas été démontré et que celle-ci travaille sans doute pour une société concurrente qui propose une solution logicielle similaire.
10. Le 6 septembre 2023, les parties sont informées que la Chambre Contentieuse procède d'office à la fixation d'une audition dont la date est fixée au 23 novembre 2023.
11. Le 6 septembre 2023, la Chambre Contentieuse reçoit un e-mail de la plaignante l'informant que la plainte n'est plus d'application, car plusieurs plateformes de prise de rendez-vous médicaux utilisent à présent le numéro de Registre national de manière à ce que les médecins puissent relier leurs patients aux plateformes de dossiers médicaux.
12. Le 27 septembre 2023, la Chambre Contentieuse répond au message de la plaignante en lui indiquant que malgré le retrait de sa plainte, il a été décidé de poursuivre l'examen de la plainte. Ce qui prévaut à cet égard est qu'une fois saisie, la Chambre Contentieuse est habilitée à examiner le respect du RGPD et à veiller à son application effective en toute indépendance, et ce malgré que la plainte ait été retirée par le plaignant ou soit devenue sans objet.
13. Le 26 octobre 2023, la date de l'audition est reportée au 14 décembre 2023.

¹ Software as a Service.

14. Le 11 décembre 2023, la plaignante informe la Chambre Contentieuse qu'elle ne sera pas présente à l'audition.
15. Le 14 décembre 2023, le défendeur est entendu par la Chambre Contentieuse. Bien qu'ayant été dûment convoquée, la plaignante ne participe pas à l'audition.
16. Le 21 décembre 2023, le procès-verbal de l'audition est soumis aux parties.
17. Le 22 décembre 2023, la Chambre Contentieuse reçoit du défendeur deux remarques relatives au procès-verbal qu'elle décide de reprendre dans sa délibération.

II. Motivation

a) Intérêt de la plaignante

18. Le défendeur fait remarquer que la plaignante semble poursuivre d'autres finalités, à savoir acquérir une connaissance et une compréhension de l'entreprise et des activités du défendeur. Elle ne cherche pas à remédier au préjudice qu'elle aurait subi en tant que personne concernée. Le défendeur fait valoir à cet égard qu'à aucun moment, la plaignante n'a contacté la personne de contact chargée de la protection de la vie privée au sein de son organisation, mais qu'elle a par contre décidé d'introduire immédiatement une plainte, en omettant de démontrer en quoi elle pourrait être lésée sur le plan de la protection des données.
19. La Chambre Contentieuse déclare qu'en principe, elle ne vérifie pas la finalité du plaignant lorsqu'une plainte est introduite. Elle prend toutefois en considération la mesure dans laquelle un plaignant a un intérêt. En ce qui concerne l'intérêt dans le chef de la plaignante, la Chambre Contentieuse attire l'attention sur ce qui suit :
20. L'article 58 de la LCA dispose que : "*Toute personne peut déposer une plainte ou une requête écrite, datée et signée auprès de l'Autorité de protection des données*". Conformément à l'article 60, alinéa 2 de la LCA "*Une plainte est recevable lorsqu'elle :*
 - *est rédigée dans l'une des langues nationales ;*
 - *contient un exposé des faits et les indications nécessaires pour identifier le traitement sur lequel elle porte ;*
 - *relève de la compétence de l'Autorité de protection des données*".
21. Les travaux préparatoires de la LCA disposent que : "*Toute personne peut déposer une plainte ou une requête auprès de l'Autorité de protection des données : des personnes physiques, mais également des personnes morales, des associations ou des institutions qui souhaitent dénoncer une infraction supposée au règlement. Une plainte ou une requête adressée à l'Autorité de protection des données doit être écrite, datée et signée par la*

personne compétente en la matière. Une requête doit être interprétée dans le sens le plus large du mot (demande d'information ou d'explication, demande de médiation, ...)"².

22. La LCA n'exclut pas qu'une autre personne que la personne concernée ou la personne mandatée par celle-ci, au sens de l'article 220 de la loi du 30 juillet 2018 *relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel* puisse introduire une plainte auprès de l'Autorité.
23. Bien que le RGPD considère la 'plainte' du point de vue de la personne concernée, en imposant des obligations aux autorités de contrôle lorsqu'une personne introduit une plainte (voir les articles 57, 1.f) et 77 du RGPD), le RGPD n'empêche pas que le droit national donne la possibilité à d'autres personnes que les personnes concernées d'introduire une plainte auprès de l'autorité de contrôle nationale. La possibilité d'une telle saisine correspond d'ailleurs aux missions confiées par le RGPD aux autorités de contrôle. À cet égard et de façon générale, chaque autorité de contrôle : veille au contrôle de l'application du RGPD et au respect de celui-ci (art. 57.1.a) du RGPD) et s'acquitte de toute autre mission relative à la protection des données à caractère personnel (art. 57.1.v) du RGPD)³.
24. La Chambre Contentieuse estime à cet égard que l'article 58 de la LCA donne à toute personne la possibilité d'introduire une plainte, à condition qu'elle y ait un intérêt suffisant, conformément aux dispositions susmentionnées du RGPD.
25. La condition est toutefois que le plaignant justifie d'un intérêt suffisant. À cet égard, la Chambre Contentieuse souligne que sur la base des pièces du dossier, la plaignante mentionne uniquement le fait qu'elle a consulté le site Internet [...], lequel utilise le système de prise de rendez-vous en ligne du défendeur. Ce simple fait amène la plaignante à supposer que le numéro de Registre national est conservé dans la base de données du défendeur, sans joindre le moindre document démontrant que la plaignante est affectée dans la protection de ses données à caractère personnel. Le site Internet en question peut en effet être consulté librement par tout le monde, ce qui permet à la plaignante d'alléguer, sur cette simple base et sans qu'aucun traitement de données ne soit requis à cet effet, d'éventuelles violations de la sécurité des données à caractère personnel par le défendeur et une éventuelle utilisation inadmissible d'informations, en particulier du numéro de Registre national.
26. Compte tenu du fait que la plaignante ne démontre pas que le défendeur traite des données à caractère personnel la concernant et qu'elle ne prouve pas non plus un intérêt suffisamment concret pour pouvoir introduire une plainte, la Chambre Contentieuse constate de surcroît que la plaignante ne dispose pas non plus de la qualité pour pouvoir

² *Doc. parl.*, Chambre des représentants, 2016-2017, DOC 54 2648/001, p. 40 (remarque sur l'article 58 du projet de loi initial).

³ Dans sa décision du 8 juin 2020, la Chambre Contentieuse a déjà admis, sous des conditions très strictes, qu'une personne autre que la personne concernée introduise une plainte (Décision quant au fond 30/2020, publiée sur le site Internet de l'APD).

introduire une plainte et que par conséquent, toute la procédure est entachée par l'absence non seulement d'un intérêt mais aussi de qualité dans le chef de la plaignante.

b) Qualité du défendeur

27. Afin de pouvoir déterminer les obligations qui incombent au défendeur en vertu du RGPD, il convient de déterminer au préalable en quelle qualité le défendeur intervient par rapport au traitement de données qui fait l'objet de la plainte. Le point crucial à cet égard est de déterminer si le défendeur agit en tant que responsable du traitement (article 4.7) du RGPD⁴) ou en tant que sous-traitant (article 4.8) du RGPD⁵).
28. Le rapport d'inspection spécifie que le défendeur a fait l'objet de l'enquête en sa qualité de sous-traitant vis-à-vis des données à caractère personnel des clients pour lesquels il traite des données à caractère personnel. Le défendeur argumente également lui-même qu'il intervient uniquement en tant que sous-traitant, pas en tant que responsable du traitement. La Chambre Contentieuse vérifie si le point de départ selon lequel le défendeur doit uniquement être considéré comme un sous-traitant correspond à l'interprétation (large) de la notion de responsable du traitement par la Cour de justice⁶ et l'European Data Protection Board (EDPB ou Comité européen de la protection des données), en particulier dans les Lignes directrices 07/2020 concernant la notion de responsable du traitement.
29. Le RGPD définit un "responsable du traitement" comme une entité qui, seule ou conjointement avec d'autres, détermine les finalités et les moyens du traitement des données à caractère personnel⁷. Cette définition doit être comprise à la lumière de la finalité du législateur qui consiste à attribuer la responsabilité principale de la protection des données à caractère personnel à l'entité qui exerce réellement un contrôle sur le traitement

⁴ Article 4 du RGPD :

"Aux fins du présent règlement, on entend par :

[...]

7) "responsable du traitement" : la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement ; lorsque les finalités et les moyens de ce traitement sont déterminés par le droit de l'Union ou le droit d'un État membre, le responsable du traitement peut être désigné ou les critères spécifiques applicables à sa désignation peuvent être prévus par le droit de l'Union ou par le droit d'un État membre ;"

⁵ Article 4 du RGPD :

"Aux fins du présent règlement, on entend par :

[...]

8) "sous-traitant" : la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement ;"

⁶ Voir e.a. CJUE, Arrêt du 10 juillet 2018, Jehovan todistajat, C-25/17, ECLI:EU:C:2018:551, pt 66, et plus récemment l'arrêt du 7 mars 2024, IAB Europe, C-604/22, ECLI:EU:C:2024:214, pt 55.

⁷ Art. 4.7) du RGPD

de données. Ceci implique qu'il ne faut pas seulement tenir compte de la qualification juridique mais aussi de la réalité factuelle⁸.

30. L'EDPB a précisé que le concept de responsable du traitement se fonde sur l'influence du responsable du traitement sur le traitement, basée sur une compétence décisionnelle ou un contrôle sur les activités de traitement. Un tel contrôle peut résulter de dispositions légales, d'une compétence implicite ou se fonder sur l'exercice d'une influence de fait⁹. En substance, la détermination des finalités et des moyens correspond à la détermination respectivement du pourquoi et du comment du traitement : pour une activité de traitement particulière, le responsable du traitement est celui qui exerce cette influence sur le traitement de données à caractère personnel et qui détermine donc pourquoi le traitement a lieu (c'est-à-dire à quelles fins ou pourquoi) et comment cet objectif sera atteint (c'est-à-dire quels moyens doivent être utilisés pour atteindre l'objectif)¹⁰.
31. La compétence consistant à déterminer les moyens et les finalités des activités de traitement peut tout d'abord être liée au rôle fonctionnel d'une organisation¹¹. En outre, la responsabilité peut être attribuée sur la base de dispositions contractuelles entre les parties concernées, bien que ces dispositions ne soient pas toujours déterminantes¹², ou sur la base d'une appréciation du contrôle factuel d'une partie. Ainsi, la détermination des moyens et des finalités peut résulter d'une influence déterminante sur le traitement, plus précisément sur la raison pour laquelle un traitement est effectué d'une certaine manière¹³.
32. Dans son arrêt sur les Témoins de Jéhovah¹⁴, la Cour de justice donne une explication détaillée concernant la notion de responsable du traitement. Cet arrêt souligne que la définition de responsable du traitement doit être interprétée de manière large afin d'assurer "une protection efficace et complète des personnes concernées"¹⁵, et qu'il n'est pas

⁸ L. A. BYGRAVE & L. Tosoni, "Article 4(7). Controller" in *The EU General Data Protection Regulation. A commentary*, Oxford University Press, 2020, p. 148.

⁹ EDPB – Lignes directrices 07/2020 concernant les notions de responsable du traitement et de sous-traitant dans le RGPD, v 2.0, 2021, paragraphe 20 e.s.

¹⁰ *Ibid.*, paragraphe 35.

¹¹ D. De Bot, *De toepassing van de Algemene Verordening Gegevensbescherming in de Belgische context*, Wolters Kluwer, 2020, paragraphes 362.

¹² D. De Bot, *De toepassing van de Algemene Verordening Gegevensbescherming in de Belgische context*, Wolters Kluwer, 2020, paragraphes 363-365.

¹³ EDPB – Lignes directrices 07/2020 concernant les notions de responsable du traitement et de sous-traitant dans le RGPD, v 2.0, 2021, paragraphe 20.

¹⁴ CJUE, Arrêt du 10 juillet 2018, *Jehovan todistajat* C-25/17, ECLI:EU:C:2018:551.

¹⁵ Arrêt CJUE du 13 mai 2014, *Google Spain en Google e.a.*, C-131/12, ECLI:EU:C:2014:317, paragraphe 34 ; voir également la discussion concernant la portée de la notion dans C. DOCKSEY et H. HIJMANS, "The Court of Justice as a Key Player in Privacy and Data Protection", *European Data Protection Law Review*, 2019, Vol. 3, (300)304.

nécessaire d'avoir accès aux données à caractère personnel faisant l'objet du traitement pour être pris en considération en tant que responsable du traitement¹⁶.

33. Les éléments déterminants pour établir si le traitement de données a lieu en qualité de responsable du traitement ou de sous-traitant sont les finalités et les moyens, plus précisément la mesure dans laquelle il existe un pouvoir de décision à ce sujet.
34. Concrètement, le traitement de données est effectué en l'espèce par le défendeur à l'aide d'une application logicielle qui consiste en un système de prise de rendez-vous basé sur une technologie Internet. Afin d'évaluer l'impact du défendeur sur la finalité et les moyens, il est d'abord nécessaire de comprendre le fonctionnement de cette application. Celle-ci fonctionne comme suit :
 - a. Le patient surfe sur le site Internet du cabinet médical ou utilise l'application ;
 - b. Le patient s'identifie dans le système d'agenda en ligne. L'utilisateur de l'application, en l'espèce le prestataire de soins, choisit lui-même les modalités de connexion du patient, à savoir via 1) un nom d'utilisateur et un mot de passe ; 2) les nom, prénom et date de naissance ; 3) l'e-ID ; 4) le numéro de Registre national ou 5) un compte de réseau social ;
 - c. Le patient choisit le médecin avec qui il souhaite prendre un rendez-vous ;
 - d. Le patient choisit éventuellement un type de rendez-vous ;
 - e. Le patient choisit le créneau horaire souhaité ;
 - f. Le patient ajoute, à titre optionnel, des remarques complémentaires ;
 - g. Le patient confirme son rendez-vous.
35. Le défendeur contrôle ensuite si les données à caractère personnel en question du patient concerné figurent dans la base de données du prestataire de soins. Si tel est le cas, le patient peut prendre un rendez-vous. Si ce n'est pas le cas, soit le patient peut s'enregistrer manuellement, soit l'accès lui est refusé si le prestataire de soins ne souhaite pas accepter de nouveaux patients. L'enquête menée par le Service d'Inspection a permis d'établir que le défendeur ne transfère aucune donnée à caractère personnel de patients aux gestionnaires de médias sociaux évoqués.
36. Sur la base des éléments de ce dossier, la Chambre Contentieuse constate que la finalité poursuivie consiste à disposer d'un système d'agenda en ligne permettant de prendre des rendez-vous et de recevoir des rappels de rendez-vous, d'échanger des données avec d'autres applications et de prendre des rendez-vous de façon entièrement automatisée par téléphone. Cette finalité découle de la nécessité pour le prestataire de soins de pouvoir

¹⁶ CJUE, Arrêt du 10 juillet 2018, *Tietosuojavaltuutettu et Jehovan todistajat – uskonnollinen yhdyskunta*, C-25/17, ECLI:EU:C:2018:551. Voir également EDPB - Lignes directrices 07/2020 concernant les notions de responsable du traitement et de sous-traitant dans le RGPD, v 2.0, 2021, paragraphe 45.

enregistrer les rendez-vous avec les patients de manière efficace et performante. Cela signifie que la finalité est déterminée de manière entièrement autonome par le prestataire de soins et que le système d'agenda en ligne du défendeur constitue simplement un moyen d'atteindre cette finalité. À cet égard, il est établi que seuls les prestataires de soins qui considèrent que l'application proposée par le défendeur, avec les possibilités offertes par le système d'agenda en ligne pour l'enregistrement des rendez-vous avec les patients, répond à leurs besoins concrets, recourront effectivement également au défendeur et concluront un contrat avec lui. Le prestataire de soins ne décide donc pas uniquement de la finalité, mais décide entièrement seul du moyen qui est selon lui le plus adéquat pour atteindre la finalité qu'il poursuit.

37. Dans ce contexte, le défendeur joue un rôle purement intermédiaire dans le sens où il se contente de présenter et de proposer les différentes fonctionnalités de l'application. C'est toutefois exclusivement le prestataire de soins qui, en fonction de la finalité qu'il poursuit, choisit parmi les options offertes par l'application, les fonctionnalités qu'il souhaite utiliser. Étant donné que tant la finalité que le moyen de l'atteindre sont déterminés exclusivement par le prestataire de soins, il convient dès lors de lui attribuer la qualité de responsable du traitement.
38. Le défendeur, par contre, satisfait aux deux conditions principales¹⁷ pour être qualifié de sous-traitant au sens de l'article 4. 8) du RGPD, à savoir :
 - a) il s'agit d'une *personne morale distincte*, indépendante par rapport au responsable du traitement, en l'espèce le prestataire de soins, et
 - b) cette personne traite les données à caractère personnel *pour le compte* du responsable du traitement.
39. Les prestataires de soins, généralement un cabinet de prestataires de soins, décident de sous-traiter l'activité consistant en l'enregistrement des rendez-vous avec les patients au défendeur, une organisation externe totalement indépendante du cabinet dont font partie les prestataires de soins. Le défendeur dispose également de la personnalité morale requise, étant donné que ce dernier a adopté la forme d'une société à responsabilité limitée.
40. Le contrat de sous-traitance que le défendeur a fourni dans le cadre de l'enquête du Service d'Inspection montre que l'activité de traitement est effectuée moyennant la stricte obligation pour le défendeur de l'exécuter conformément aux instructions écrites du prestataire de soins et uniquement d'après ces instructions. La Chambre Contentieuse constate qu'à cet égard, il n'existe pas la moindre marge pour le défendeur de traiter les données à caractère personnel obtenues pour une quelconque autre finalité propre. Il y est

¹⁷ EDPB – Lignes directrices 07/2020 concernant les notions de responsable du traitement et de sous-traitant dans le RGPD, v 2.0, 2021, paragraphe 73 - 84.

aussi explicitement indiqué que le défendeur ne traitera les données à caractère personnel pour aucune autre finalité que celle qui a été définie par le prestataire de soins et en ce sens, l'exigence reprise à l'article 28.10 du RGPD pour être considéré comme sous-traitant est satisfaite. En effet, toute finalité propre à l'égard des données obtenues est totalement absente dans le chef du défendeur qui traite ces données uniquement pour le compte du prestataire de soins.

41. La qualité de sous-traitant du défendeur est encore confirmée par le fait que l'activité de traitement concrète du défendeur, en tant que prestataire de services qui traite les données à caractère personnel du patient dans le cadre de sa relation avec le prestataire de soins afin de permettre l'enregistrement d'un rendez-vous entre patient et prestataire de soins, a lieu pour le compte du prestataire de soins qui a le contrôle absolu du traitement de données. À cet égard, la nature du service est primordiale en ce sens que, pour être qualifié de sous-traitant, le service presté doit être spécifiquement axé sur le traitement de données à caractère personnel ou le traitement effectué doit constituer un aspect essentiel de ce service. L'application logicielle mise à disposition par le défendeur est essentiellement axée sur le traitement de données à caractère personnel de patients telles que fournies par le prestataire de soins et qui sont nécessaires à l'enregistrement de rendez-vous, et uniquement de rendez-vous, avec le prestataire de soins concerné sans que le défendeur ne propose dans ce contexte de gestion de dossiers de données de santé et sans qu'il ait la moindre influence sur la détermination des finalités et des moyens du traitement.
42. Vu que la Chambre Contentieuse estime qu'il est établi que le défendeur agit en tant que sous-traitant, ceci a des conséquences pour les obligations relatives à la protection des données qui en découlent. Les constatations du Service d'Inspection doivent dès lors être examinées à la lumière de cet élément.

c) Obligations du défendeur

1° Registre des activités de traitement

43. Sur la base des deux registres d'activités de traitement transmis par le défendeur, le Service d'Inspection a constaté que les coordonnées du responsable du traitement pour le compte duquel le défendeur agit en tant que sous-traitant étaient manquantes, ce qui n'est pas conforme à l'article 30.2.a) du RGPD. Le Service d'Inspection ajoute à cela que la lisibilité des deux registres est entravée par les nombreux renvois aux annexes pour des clarifications.
44. Le défendeur avance que la constatation de l'absence des coordonnées du responsable du traitement dans le fichier informatique contenant les informations relatives aux éléments essentiels du registre des activités de traitement ne peut pas conduire à la constatation d'une violation de l'article 30. 2.a) du RGPD, vu que les coordonnées du responsable du

traitement étaient mentionnées dans la lettre qui accompagnait le registre des activités de traitement. La lettre d'accompagnement et le registre des activités de traitement doivent être lus conjointement, d'après le défendeur.

45. En ce qui concerne le manque de clarté du registre des activités de traitement, le défendeur fait valoir qu'il est propre à la mise à disposition de données d'utiliser plusieurs tableaux liés formant des clusters. Le défendeur indique qu'il a choisi de subdiviser le registre en plusieurs niveaux au moyen de renvois aux annexes, car le fait de donner accès à toutes les informations dans un seul tableau aurait précisément pour conséquence de rendre le registre inintelligible. À cet égard, le défendeur met l'accent sur la finalité du registre des activités de traitement qui n'est pas destiné à la personne concernée, mais bien à l'Autorité de protection des données (ci-après "l'APD") qui l'utilise comme un 'outil' de mise à disposition des informations lui permettant de vérifier quelles sont les activités de traitement.
46. Compte tenu du fait que suite à la demande du Service d'Inspection de présenter le registre des activités de traitement, le défendeur a fourni toutes les informations, y compris les coordonnées du responsable du traitement pour le compte duquel le défendeur agit en tant que sous-traitant, afin de permettre au Service d'Inspection d'accomplir sa mission de contrôle, il en résulte que la finalité de l'article 30. 2 du RGPD est atteinte. Le registre des activités de traitement vise en effet à permettre à l'APD, dont le Service d'Inspection fait partie, de contrôler les activités de traitement. La possibilité d'exercer ce contrôle n'a à aucun moment été compromise par un quelconque manque d'information, de sorte que le défendeur n'a donc aucunement failli à son obligation de collaborer avec l'APD, puisqu'il a fourni spontanément au Service d'Inspection, à la première demande, le registre des activités de traitement accompagné des coordonnées du responsable du traitement pour le compte duquel les données à caractère personnel étaient traitées¹⁸. Bien qu'il soit préférable que les coordonnées du responsable du traitement pour le compte duquel le sous-traitant effectue le traitement de données figurent également dans le registre des activités de traitement proprement dit, afin que le défendeur respecte pleinement les données à inclure obligatoirement dans le registre, la Chambre Contentieuse considère que le défendeur a respecté son obligation de fournir toutes les informations requises à l'article 30.2 du RGPD.
47. En ce qui concerne la manière dont les informations sont reprises dans le registre des activités de traitement, la Chambre Contentieuse fait remarquer que le RGPD n'impose aucune exigence de forme intrinsèque qui interdirait l'accès stratifié aux informations en

¹⁸ Voir également à cet égard le considérant 82 du RGPD : "Afin de démontrer qu'il respecte le présent règlement, le responsable du traitement ou le sous-traitant devrait tenir des registres pour les activités de traitement relevant de sa responsabilité. Chaque responsable du traitement et sous-traitant devrait être tenu de coopérer avec l'autorité de contrôle et de mettre ces registres à la disposition de celle-ci, sur demande, pour qu'ils servent au contrôle des opérations de traitement."

faisant référence à des annexes. Le Service d'Inspection observe que les nombreux renvois aux annexes entravent la lisibilité du registre des activités de traitement, mais sans constater que cela empêcherait le Service d'Inspection d'obtenir une vue d'ensemble des activités de traitement effectuées par le défendeur. Le Service d'Inspection a donc bien pu remplir sa mission de contrôle.

48. Compte tenu de ce qui précède, la Chambre Contentieuse considère qu'**aucune violation de l'article 30. 2 du RGPD** n'a été commise.

2° Délégué à la protection des données

49. Le rapport du Service d'Inspection indique que, contrairement à ce qu'avance le défendeur, un délégué à la protection des données aurait dû être désigné. Selon le Service d'Inspection, le défendeur traite en effet à grande échelle des données à caractère personnel de patients, y compris des données de santé, et le système de prise de rendez-vous en ligne exige un suivi régulier et systématique des rendez-vous que ces patients prennent avec leur médecin, ce qui met le défendeur dans l'obligation de désigner un délégué à la protection des données, conformément à l'article 37. 1 du RGPD.

50. Le défendeur réfute le suivi régulier et systématique à grande échelle des personnes concernées (article 37.1.b) du RGPD) en objectant qu'il n'est aucunement établi que les rendez-vous soient régulièrement pris par le biais de l'application logicielle du défendeur, vu que le patient n'est pas obligé de l'utiliser. Le patient est en effet libre de se rendre à la consultation sans rendez-vous ou de prendre un rendez-vous par téléphone, sans qu'il y ait une intervention du défendeur. Il est également possible, selon le défendeur, qu'un patient consulte un médecin au maximum 1 ou 2 fois par an, de sorte qu'il ne peut pas non plus être question de régularité.

51. Cette analyse est pertinente, au regard de l'article 37.1.b) du RGPD qui exige un suivi régulier et systématique. Les notions de "régulier" et de "systématique" ne sont pas définies dans le RGPD, mais une interprétation en est toutefois donnée dans les Lignes directrices *concernant les délégués à la protection des données*¹⁹. L'interprétation possible donnée à la notion de "régulier" est :

- continu ou se produisant à intervalles réguliers au cours d'une période donnée ;
- récurrent ou se répétant à des moments fixes ;
- ayant lieu de manière constante ou périodique

La notion de "systématique" est définie comme suit :

¹⁹ Ces Lignes directrices du Groupe de travail Article 29 ont été approuvées le 13 décembre 2016, révisées pour la dernière fois et approuvées le 5 avril 2017 et ratifiées par le Comité européen de la protection des données.

- se produisant conformément à un système ;
- préétabli, organisé ou méthodique ;
- ayant lieu dans le cadre d'un programme général de collecte de données ;
- effectué dans le cadre d'une stratégie.

52. La Chambre Contentieuse déduit des exemples donnés, dans les Lignes directrices susmentionnées, de traitements pouvant constituer un suivi régulier et systématique des personnes concernées²⁰ que le suivi comportemental n'est pas isolé, mais qu'il s'accompagne toujours d'une finalité propre. Selon la Chambre Contentieuse, l'enregistrement d'un rendez-vous entre un prestataire de soins et un patient s'en distingue en ce sens qu'aucune autre finalité n'est poursuivie que la simple prise d'un rendez-vous, laquelle est absolument sans lien avec un quelconque contrôle du comportement du patient concerné. Les données obtenues sont exclusivement utilisées pour fixer un rendez-vous. Aucun élément n'indique en effet que ces mêmes données sont analysées pour y associer la moindre conséquence ou finalité, de sorte que l'on ne peut dès lors pas conclure qu'elles viseraient à soumettre les patients concernés à une forme quelconque de suivi régulier ou systématique.

53. En ce qui concerne le caractère à grande échelle du traitement de catégories particulières de données à caractère personnel au sens de l'article 9 du RGPD, le défendeur souligne tant dans les conclusions en réplique que pendant l'audition qu'il n'y a pas de gestion de dossier de données de santé, mais que l'application rend simplement possible la prise d'un rendez-vous, ce qui permet tout au plus de déduire que la personne concernée est peut-être malade. Le caractère à grande échelle du traitement de données est également réfuté par le défendeur, qui souligne que le traitement de données dont il est question se distingue du traitement de données par un hôpital ou un organisme assureur, qui doit bel et bien être qualifié comme étant à grande échelle. Vu sous cet angle, le défendeur estime que la désignation d'un délégué à la protection des données n'est donc pas requise.

54. Afin de déterminer si le défendeur doit ou non disposer d'un délégué à la protection des données, la Chambre Contentieuse a examiné les éléments portés à sa connaissance dans le cadre du présent dossier à la lumière des Lignes directrices *concernant les délégués à la protection des données*²¹. Étant donné que conformément à l'article 37.1 b) et c) du RGPD, le traitement de données doit être effectué "à grande échelle", mais que l'interprétation

²⁰ Exemples d'activités pouvant constituer un suivi régulier et systématique des personnes concernées : exploitation d'un réseau de télécommunications; fourniture de services de télécommunications ; recyclage par courrier électronique ; activités de marketing fondées sur les données ; profilage et notation à des fins d'évaluation des risques (par exemple, aux fins de l'évaluation du risque de crédit, de l'établissement des primes d'assurance, de la prévention de la fraude ou de la détection du blanchiment d'argent) ; géolocalisation, par exemple, par des applications mobiles; programmes de fidélité ; publicité comportementale; surveillance des données sur le bien-être, la santé et la condition physique au moyen de dispositifs portables ; systèmes de télévision en circuit fermé ; dispositifs connectés tels que les voitures et compteurs intelligents, la domotique, etc.

²¹ https://ec.europa.eu/newsroom/just/document.cfm?doc_id=44100.

qu'il convient de donner à ces termes n'y est pas davantage définie, les Lignes directrices susmentionnées fournissent un certain nombre de facteurs permettant de déterminer si un traitement est mis en œuvre à grande échelle ou non. Ces facteurs sont les suivants :

- le nombre de personnes concernées, soit en valeur absolue, soit en valeur relative par rapport à la population concernée
- le volume de données et/ou le spectre des données traitées
- la durée, ou la permanence, des activités de traitement des données
- l'étendue géographique de l'activité de traitement.

55. Comme dans le considérant 91 du RGPD, les Lignes directrices *concernant les délégués à la protection des données* indiquent également qu'un traitement de données à caractère personnel ne peut pas être considéré comme un traitement à grande échelle s'il implique le traitement de données à caractère personnel de patients ou de clients par un médecin ou un autre professionnel de la santé exerçant à titre individuel. D'après le considérant 91 du RGPD, un tel traitement ne doit donc pas être considéré comme un traitement à grande échelle dans le sens d'un traitement visant à traiter un volume considérable de données à caractère personnel au niveau régional, national ou supranational, qui peut affecter un nombre important de personnes concernées et qui est susceptible d'engendrer un risque élevé, par exemple, en raison de leur caractère sensible, lorsque, en conformité avec l'état des connaissances technologiques, une nouvelle technique est appliquée à grande échelle, ou au sens d'autres opérations de traitement qui engendrent un risque élevé pour les droits et libertés des personnes concernées, en particulier lorsque, du fait de ces opérations, il est plus difficile pour ces personnes d'exercer leurs droits. Dans le cas présent, la Chambre Contentieuse tient également compte du fait qu'en sa qualité de sous-traitant, le défendeur effectue le traitement de données pour le compte du prestataire de soins. Le fait que le prestataire de soins confie le traitement de données à un sous-traitant n'a pas d'incidence sur l'absence de caractère "à grande échelle" du traitement. En outre, le défendeur traite uniquement les données d'identification du patient qui sont pertinentes pour pouvoir fixer un rendez-vous dans l'agenda du prestataire de soins et qui garantissent l'identification unique sans qu'une quelconque gestion de dossier de données de santé y soit associée. Le fait de déduire de la prise de rendez-vous avec un prestataire de soins qu'un patient est peut-être malade ne suffit pas pour qualifier de risqué ce traitement dont la finalité se limite à la prise d'un rendez-vous.

56. Par conséquent, la Chambre Contentieuse considère qu'**aucune violation de l'article 37.1 du RGPD** n'a été commise.

d) Utilisation du numéro de Registre national et mesures de sécurité

57. En ce qui concerne l'utilisation du numéro de Registre national par le défendeur, le rapport du Service d'Inspection se limite à indiquer que l'utilisation ou non du numéro de Registre national dans le système de prise de rendez-vous en ligne du défendeur dépend du choix qui est fait à cet égard par le client, à savoir le prestataire de soins ou le cabinet de prestataires de soins, du défendeur, vu que c'est le client qui choisit les modalités de connexion du patient au système. Le Service d'Inspection ne constate pas une quelconque infraction concernant l'utilisation du numéro de Registre national, mais se limite à la constatation que le défendeur traite le numéro de Registre national pour le compte de ses clients.
58. La Chambre Contentieuse estime que la constatation du Service d'Inspection selon laquelle le client choisit la méthode de connexion pour le patient, ce choix ne revenant donc pas au défendeur, vaut confirmation que le client, à savoir le prestataire de soins, est le responsable du traitement (voir plus haut le point 'b) Qualité du défendeur'), et que ce dernier doit disposer de l'autorisation d'utiliser le numéro de Registre national s'il décide que le patient peut se connecter au moyen de son numéro de Registre national. Le défendeur ne peut dès lors appliquer cette méthode de connexion et utiliser ce numéro que dans la mesure où le prestataire de soins est lui-même autorisé à utiliser le numéro de Registre national en application de l'article 8 de la loi du 8 août 1983 *organisant un registre national des personnes physiques*. Ceci est possible sur la base d'une législation qui prévoit l'utilisation du numéro de Registre national ou sur la base d'une autorisation d'utilisation de ce numéro. Dans la mesure nécessaire, la Chambre Contentieuse rappelle qu'une délibération accordant une autorisation doit être considérée comme une disposition plus spécifique en droit national au sens des articles 6.2 et 6.3 du RGPD, qui a donc une portée juridique.
59. Bien que ce point ne fasse pas l'objet de la plainte et ne soit donc pas en cause, mais qu'il est bel et bien essentiel pour déterminer dans quelle mesure et sous quelles conditions le défendeur peut traiter le numéro de Registre national, la Chambre Contentieuse attire l'attention sur le fait que les prestataires de soins avec lesquels le patient entretient une relation thérapeutique sont autorisés à utiliser le numéro de Registre national du patient concerné pour notamment accéder au dossier médical global. Le numéro de Registre national constitue à cet égard la clé d'une identification unique dont il faut souligner l'importance, compte tenu de la santé du patient qui est au cœur du processus, tout risque de confusion d'identité devant être exclu. Sur la base de ce qui précède, la Chambre Contentieuse conclut que le défendeur qui traite le numéro de Registre national dans sa base de données sous la forme de son hachage, pour le compte du responsable du traitement, à savoir le prestataire de soins, le fait de façon licite dans la mesure où il satisfait à toutes les obligations imposées par le RGPD à un sous-traitant, y compris la conclusion

d'un contrat de sous-traitance. Le Service d'Inspection a explicitement constaté à cet égard dans son rapport que le défendeur n'a commis **aucune violation de l'article 28.3 du RGPD**²².

60. Conformément à l'article 28.1 du RGPD, le défendeur qui intervient en tant que sous-traitant doit offrir des garanties suffisantes quant à l'application de mesures techniques et organisationnelles appropriées de manière à ce que le traitement réponde aux exigences du RGPD et à ce que la protection des droits de la personne concernée soit garantie. Le Service d'Inspection a obtenu des informations du défendeur afin de pouvoir évaluer si celui-ci satisfait aux exigences de l'article 32 du RGPD, mais considère que cette réponse contient une description formulée de manière très générale et une liste de mesures qui auraient été prises, sans joindre la copie demandée des documents. Sur la base de ce qui précède, le Service d'Inspection constate qu'il y a violation de l'article 32.1 du RGPD et de l'article 31 du RGPD.

61. Le défendeur soutient avoir bel et bien expliqué en toute transparence comment l'application fonctionne et où les données à caractère personnel sont conservées. Il renvoie à cet effet à sa réponse par courrier du 29 avril 2020. Selon le défendeur, ces éléments, ainsi que la liste détaillée des mesures techniques et organisationnelles, apportent au Service d'Inspection une compréhension suffisante de la situation. En ce qui concerne la remarque formulée dans le rapport du Service d'Inspection selon laquelle le défendeur aurait pu fournir

²² Article 28.3. "Le traitement par un sous-traitant est régi par un contrat ou un autre acte juridique au titre du droit de l'Union ou du droit d'un État membre, qui lie le sous-traitant à l'égard du responsable du traitement, définit l'objet et la durée du traitement, la nature et la finalité du traitement, le type de données à caractère personnel et les catégories de personnes concernées, et les obligations et les droits du responsable du traitement. Ce contrat ou cet autre acte juridique prévoit, notamment, que le sous-traitant :

a) ne traite les données à caractère personnel que sur instruction documentée du responsable du traitement, y compris en ce qui concerne les transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale, à moins qu'il ne soit tenu d'y procéder en vertu du droit de l'Union ou du droit de l'État membre auquel le sous-traitant est soumis; dans ce cas, le sous-traitant informe le responsable du traitement de cette obligation juridique avant le traitement, sauf si le droit concerné interdit une telle information pour des motifs importants d'intérêt public ;

b) veille à ce que les personnes autorisées à traiter les données à caractère personnel s'engagent à respecter la confidentialité ou soient soumises à une obligation légale appropriée de confidentialité ;

c) prend toutes les mesures requises en vertu de l'article 32 ;

d) respecte les conditions visées aux paragraphes 2 et 4 pour recruter un autre sous-traitant ;

e) tient compte de la nature du traitement, aide le responsable du traitement, par des mesures techniques et organisationnelles appropriées, dans toute la mesure du possible, à s'acquitter de son obligation de donner suite aux demandes dont les personnes concernées le saisissent en vue d'exercer leurs droits prévus au chapitre III ;

f) aide le responsable du traitement à garantir le respect des obligations prévues aux articles 32 à 36, compte tenu de la nature du traitement et des informations à la disposition du sous-traitant ;

g) selon le choix du responsable du traitement, supprime toutes les données à caractère personnel ou les renvoie au responsable du traitement au terme de la prestation de services relatifs au traitement, et détruit les copies existantes, à moins que le droit de l'Union ou le droit de l'État membre n'exige la conservation des données à caractère personnel ; et

h) met à la disposition du responsable du traitement toutes les informations nécessaires pour démontrer le respect des obligations prévues au présent article et pour permettre la réalisation d'audits, y compris des inspections, par le responsable du traitement ou un autre auditeur qu'il a mandaté, et contribuer à ces audits.

En ce qui concerne le point h) du premier alinéa, le sous-traitant informe immédiatement le responsable du traitement si, selon lui, une instruction constitue une violation du présent règlement ou d'autres dispositions du droit de l'Union ou du droit des États membres relatives à la protection des données."

plus de clarté quant à ce que signifie en pratique que toutes les données sont conservées et traitées dans des centres de données certifiés ISO 27001, le défendeur explique dans la mesure nécessaire dans les conclusions que la norme ISO 27001 a été établie afin de définir les exigences pour la définition, la mise en œuvre, la tenue à jour et l'amélioration continue d'un système de gestion de la sécurité de l'information. Le système de gestion de la sécurité de l'information protège la confidentialité, l'intégrité et la disponibilité des informations en appliquant un processus de gestion des risques et garantit aux parties concernées que les risques sont gérés de façon adéquate. En marge, le défendeur attire également l'attention à cet égard sur le fait que la seule finalité et fonctionnalité de la solution SaaS²³ consiste en la prise de rendez-vous avec le médecin, de sorte que l'impact pour la personne concernée est très faible.

62. Sur la base des éléments avancés par le défendeur dans les conclusions en se référant aux pièces, la Chambre Contentieuse conclut que le défendeur a déployé les efforts nécessaires à la fois pour démontrer que les mesures techniques et organisationnelles requises ont été prises pour garantir un traitement de données sécurisé, ainsi que pour fournir les informations requises au Service d'Inspection, de sorte qu'il n'y a **pas de violation de l'article 32.1 du RGPD, ni de l'article 31 du RGPD.**

III. Publication de la décision

63. 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, de classer la présente plainte sans suite, en vertu de l'article 100, § 1^{er}, 1^o de la LCA, vu qu'aucune violation du RGPD ne peut être établie à cet égard.

En vertu de l'article 108, § 1^{er} de la LCA, cette décision peut faire l'objet d'un recours auprès de la Cour des marchés (Cour d'appel de Bruxelles) dans un délai de trente jours à compter de sa notification, avec l'Autorité de protection des données en qualité de défenderesse.

²³ Le Software as a Service (SaaS) permet aux utilisateurs de se connecter à des applications cloud et de les utiliser via Internet.

Un tel recours peut être introduit au moyen d'une requête contradictoire qui doit comporter les mentions énumérées à l'article 1034*ter* du *Code judiciaire*²⁴. La requête contradictoire doit être déposée au greffe de la Cour des marchés conformément à l'article 1034*quinquies* du *Code judiciaire*²⁵, ou via le système informatique e-Deposit de la Justice (article 32*ter* du *Code judiciaire*).

(sé.) Hielke HIJMANS

Président de la Chambre Contentieuse

²⁴ "La requête contient à peine de nullité :

1° l'indication des jour, mois et an ;

2° les nom, prénom, domicile du requérant, ainsi que, le cas échéant, ses qualités et son numéro de registre national ou numéro d'entreprise ;

3° les nom, prénom, domicile et, le cas échéant, la qualité de la personne à convoquer ;

4° l'objet et l'exposé sommaire des moyens de la demande ;

5° l'indication du juge qui est saisi de la demande ;

6° la signature du requérant ou de son avocat."

²⁵ "La requête, accompagnée de son annexe, est envoyée, en autant d'exemplaires qu'il y a de parties en cause, par lettre recommandée au greffier de la juridiction ou déposée au greffe."