Autorité de protection des données
Gegevensbeschermingsautoriteit

Chambre Contentieuse

Décision quant au fond 117/2021 du 22 octobre 2021

Numéro de dossier : DOS-2020-05264

Objet : Plainte en raison d'une connexion non sécurisée sur le site Internet d'un hôpital

La Chambre Contentieuse de l'Autorité de protection des données, constituée de Monsieur Hielke Hijmans, président, et de Messieurs Dirk Van Der Kelen et Frank De Smet, membres ;

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

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

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

Vu les pièces du dossier ;

a pris la décision suivante concernant :

Le plaignant : X, ci-après "le plaignant" ;

Le défendeur : Y, (autrefois dénommé [...], ci-après "le défendeur" ;

I. Faits et procédure

1. Le 14 novembre 2020, le plaignant a introduit une plainte auprès de l'Autorité de protection des données contre le défendeur.

2. Le plaignant est patient auprès de l'institution hospitalière du défendeur. L'objet de la plainte concerne le fait que le site Internet (...) appartenant au défendeur utilisait un formulaire de contact et un formulaire pour le service de médiation de l'hôpital. Selon le plaignant, le formulaire qui pouvait être complété par les visiteurs du site Internet serait envoyé à l'hôpital de manière non cryptée. L'utilisation d'une connexion non sécurisée permettrait à des tiers de prendre connaissance des données (de santé).

3. Le 16 novembre 2020, la plainte est déclarée recevable par le Service de Première Ligne sur la base des articles 58 et 60 de la LCA et est transmise à la Chambre Contentieuse en vertu de l'article 62, § 1er de la LCA.

4. Le 16 décembre 2020, conformément à l'article 96, § 1er 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 26 janvier 2021, l'enquête du Service d'Inspection est clôturée, le rapport est joint au dossier et celui-ci est transmis par l'inspecteur général au président de la Chambre Contentieuse (art. 91, § 1er et § 2 de la LCA). Le rapport contient des constatations concernant l'objet de la plainte et conclut qu'il est question de violations de l'article 32, paragraphes 2 et 4 du RGPD et de l'article 24, paragraphe 1 du RGPD en raison de mesures insuffisantes visant à garantir la sécurité des données à caractère personnel (particulières) qui sont traitées via le site Internet du défendeur.

6. Le rapport comporte également des constatations qui dépassent l'objet de la plainte. Le Service d'Inspection constate, dans les grandes lignes, qu'il est question de violations de l'article 24, paragraphe 1, de l'article 38, paragraphes 1 et 3 et de l'article 39 du RGPD car le délégué à la protection des données a formulé des avis au directeur général et non au conseil de direction alors que cet organe est l'organe dirigeant supérieur au sein de l'organisation du défendeur. Selon le Service d'Inspection, les informations et les avis que le délégué à la protection des données a fourni(e)s conformément à l'article 38,

paragraphe 1 et à l'article 39 du RGPD concernant les mesures de sécurité pour le site Internet (...) ne sont pas suffisamment convaincant(e)s.

7. Le 7 avril 2021, la Chambre Contentieuse décide, en vertu de l'article 95, § 1er, 1° et de l'article 98 de la LCA, que le dossier peut être traité sur le fond.

8. Sur la base du rapport du Service d'Inspection, la Chambre Contentieuse décide de scinder le dossier en deux affaires distinctes.

9. En vertu de l'article 92, 1° de la LCA, la Chambre Contentieuse prendra une décision sur le fond en ce qui concerne l'objet de la plainte.

10. En vertu de l'article 92, 3° de la LCA, la Chambre Contentieuse prendra une décision quant au fond, suite aux constatations effectuées par le Service d'Inspection en dehors du cadre de la plainte.

11. Le 7 avril 2021, les parties concernées sont informées des dispositions telles que reprises à l'article 95, § 2 ainsi qu'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.

12. Pour les constatations relatives à l'objet de la plainte, la date limite pour la réception des conclusions en réponse du défendeur a été fixée au 19 mai 2021, celle pour les conclusions en réplique du plaignant au 9 juin 2021 et enfin, celle pour les conclusions en réplique du défendeur au 30 juin 2021.

13. Le 9 avril 2021, le plaignant demande une copie du dossier (art. 95, § 2, 3° de la LCA), qui lui a été transmise le 12 avril 2021.

14. Le 11 mai 2021, le plaignant accepte de recevoir toutes les communications relatives à l'affaire par voie électronique et manifeste son intention de recourir à la possibilité d'être entendu, ce conformément à l'article 98 de la LCA.

15. Le 20 avril 2021, le défendeur accepte de recevoir toutes les communications relatives à l'affaire par voie électronique et manifeste son intention de recourir à la possibilité d'être entendu, ce conformément à l'article 98 de la LCA.

16. Le 19 mai 2021, la Chambre Contentieuse reçoit les conclusions en réponse du défendeur concernant les constatations relatives à l'objet de la plainte. Le défendeur affirme que la

protection des données à caractère personnel est suffisamment garantie grâce à l'obligation légale de secret ainsi qu'aux dispositions reprises dans le règlement de travail concernant le secret, la minimisation des données et la limitation des finalités. Par conséquent, le défendeur déclare que des données ne peuvent être traitées que dans la mesure où cela est nécessaire en vue de réaliser la finalité poursuivie. Selon le règlement de travail, le non-respect des dispositions susmentionnées est soumis à des sanctions. Selon le défendeur, le plaignant ne démontre pas que des données à caractère personnel le concernant ont été traitées via le site Internet (non sécurisé). Pour la raison qui précède, l'intérêt requis pour introduire une plainte fait défaut. Dans son rapport, le Service d'Inspection fait référence à un autre dossier au nom du défendeur. Le défendeur souligne n'avoir aucune connaissance du contenu du dossier précité. Dès lors, ce dossier n'est pas pertinent dans la cas présent.

17. Selon le défendeur, l'article 24, paragraphe 1 du RGPD a bel et bien été exécuté. Le défendeur fait tout d'abord savoir qu'il a lancé un projet ayant pour objectif final une certification ISO27001. Cette certification peut, selon le défendeur, être considérée comme la norme mondiale pour la sécurité de l'information. Ensuite, toujours selon le défendeur, il ressort des différents contrats qu'il a conclus avec des sous-traitants de données à caractère personnel qu'une analyse détaillée a été menée concernant les données à caractère personnel à traiter dans le cadre des différents contrats de sous-traitance. Le sous-traitant doit également toujours compléter un questionnaire sur la base duquel la sécurité de l'information et la protection des données sont évaluées et des mesures appropriées sont mises en œuvre.

18. En outre, selon le défendeur, le Service d'Inspection constate à tort que l'obligation de secret n'est pas respectée par l'hôpital en tant que responsable du traitement et qu'il n'a pas non plus été démontré que des violations à l'obligation de secret pouvaient effectivement être sanctionnées. Selon le défendeur, des sanctions sont bel et bien prévues et en cas de violation du secret professionnel par un médecin, un licenciement est même possible. Toujours selon le défendeur, le Service d'Inspection ne démontre pas que des données à caractère personnel, et encore moins des données de santé, sont effectivement traitées via le formulaire non sécurisé sur le site Internet. Selon lui, il n'est pas non plus démontré que des personnes non habilitées ont eu accès aux données précitées. Le défendeur affirme avoir déjà décidé de sa propre initiative le 22 décembre 2020 de supprimer les formulaires de contact. Le défendeur est une association sans but lucratif et s'appelait [...] au moment de l'introduction de la plainte. Par la suite, l'institution a étendu ses activités pour intégrer un centre de revalidation. Depuis lors, elle poursuit ses activités sous le nom Y.

19. Le défendeur considère qu'il répond également aux exigences des articles 24 et 32 du RGPD étant donné qu'il y est question des systèmes internes utilisés au sein de l'hôpital. Vu qu'il existe un lien entre le site Internet de l'hôpital d'une part et les systèmes internes d'autre part, le défendeur affirme qu'on a opté pour une authentification à deux facteurs. Selon le défendeur, il ressort notamment de ce qui précède que des mesures de sécurité suffisantes ont bel et bien été prises.

20. Une des constatations du Service d'Inspection en dehors du cadre de la plainte est que le délégué à la protection des données n'aurait émis aucun avis et n'aurait pas fait rapport à l'organe le plus élevé au sein de l'institution sur les mesures de sécurité à prendre au sein de l'hôpital. Le défendeur pense avoir à tout moment été conscient de l'importance du délégué à la protection des données et a dès lors toujours eu recours à ce dernier. En atteste, selon le défendeur, le fait que le délégué a toujours été étroitement impliqué dans les cas où un contrat de sous-traitance est conclu entre le défendeur et ses sous-traitants. Le délégué est également consulté et impliqué dans l'élaboration du nouveau site Internet afin de s'assurer que les futurs traitements réalisés via le site Internet répondent aux dispositions légales, selon le défendeur. En outre, le délégué à la protection des données fait partie de ce qu'on appelle le Comité de sécurité de l'information qui remplit un rôle de préparation et de consultation à l'égard du comité de direction concernant les questions de vie privée au sein de l'hôpital. Selon le défendeur, le directeur général est bien le pouvoir le plus élevé de la direction au sein de l'hôpital. Dès lors, il ne s'agit pas d'une violation de l'article 38, paragraphe 1 du RGPD.

21. De plus, le défendeur objecte que l'intention n'a jamais été que les formulaires de contact sur le site Internet servent à échanger des données de santé. Le dossier de patient électronique est en effet très sécurisé selon le défendeur. Il ne s'agit pas non plus d'un traitement de données à caractère personnel à grande échelle au moyen des formulaires de contact, comme l'a établi le Service d'Inspection. Le défendeur souligne qu'il ne faut pas négliger le fait qu'un formulaire pouvait être complété sur le site Internet, formulaire qui parvient auprès du service de médiation et est dès lors sans lien avec le dossier du patient. Le défendeur demande qu'il soit tenu compte de plusieurs circonstances atténuantes, à savoir qu'aucune donnée à caractère personnel n'a été consultée par des tiers de manière non autorisée et que lorsque des données à caractère personnel parviennent à l'hôpital ou sur les serveurs de l'hôpital, l'institution fait tout pour sécuriser ces données très rigoureusement.

22. Le défendeur affirme qu'il pense qu'un certificat de sécurité pour le formulaire Internet aurait dû être mis en place plus rapidement lorsque cela a été signalé. Toutefois, il n'a pas encore été prouvé qu'il avait été question d'un préjudice dans le chef de la personne concernée. Il n'y a pas eu d'accès à des données à caractère personnel par des personnes non habilitées.

23. En outre, plusieurs collaborateurs clés ont été absents en raison de la pandémie, ce qui a occasionné un retard dans l'intégration de certaines mesures. Le défendeur n'a pas été condamné précédemment pour violations du RGPD et a lancé un projet ayant pour but final l'obtention d'une certification ISO 270001 ; il demande qu'il soit tenu compte des éléments précités en tant que circonstances atténuantes.

24. Le 14 juin 2021, la Chambre Contentieuse reçoit les conclusions en réplique du plaignant, en ce qui concerne les constatations relatives à l'objet de la plainte. Le plaignant estime que la modification de la structure et de la composition de l'hôpital n'aurait pas dû conduire à ce que le site Internet ne réponde pas aux principes de protection des données. En effet, le RGPD est déjà entré en vigueur en 2018, ce qui implique que le défendeur était déjà en infraction au RGPD depuis deux ans. En réaction à l'argumentation du défendeur selon laquelle les visiteurs ne sont pas obligés d'utiliser le formulaire de contact, le plaignant objecte qu'on ne peut pas attendre des visiteurs du site Internet qu'ils prennent des précautions au moment de remplir un formulaire de contact en ligne proposé par le défendeur. Dès lors que l'on utilise un formulaire, la connexion du site Internet doit être sécurisée. Selon le plaignant, le fait que des obligations de confidentialité s'appliquent aux collaborateurs est également pertinent, dès lors que les données à caractère personnel qui sont transmises via le formulaire de contact ne sont pas sécurisées et sont exposées au risque d'être interceptées et lues par des tiers dans le trafic du réseau. Le plaignant ne partage pas la vision du défendeur selon laquelle il n'aurait aucun intérêt à introduire une plainte. Le formulaire est en effet disponible en ligne sans être sécurisé et peut être complété et envoyé par n'importe qui. Selon le plaignant, le but ne peut pas être qu'il doive rechercher les personnes concernées qui ont effectivement complété le formulaire pour leur demander ensuite d'introduire une plainte auprès de l'Autorité de protection des données.

25. Le 26 juillet 2021, les parties sont informées du fait que l'audition aura lieu le 4 octobre 2021.

26. Le 4 octobre 2021, le défendeur est entendu par la Chambre Contentieuse. En dépit d'une convocation en bonne et due forme et d'une confirmation de sa présence, le plaignant ne s'est pas présenté.

27. Le 11 octobre 2021, le procès-verbal de l'audition est soumis aux parties.

28. Le 18 octobre 2021, la Chambre Contentieuse reçoit de la part du défendeur les remarques suivantes concernant le procès-verbal : le défendeur a indiqué lors de l'audition que le nouveau site Internet était actuellement en ligne et que le délégué à la protection des données faisait rapport au comité d'audit constitué d'une représentation du Conseil d'administration.

II. Recevabilité de la plainte

29. La Chambre Contentieuse aborde tout d'abord la question de la recevabilité de la plainte. Le défendeur avance que le plaignant n'a aucun intérêt à se plaindre du site Internet et du formulaire de contact du défendeur car il ne s'agit pas d'un traitement de ses données à caractère personnel par le défendeur. Par conséquent, selon le défendeur, la plainte doit être déclarée irrecevable ou non fondée.

30. L'article 58 de la LCA dispose ce qui suit : "*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*".

31. La Chambre Contentieuse a déjà émis les considérations suivantes sur cette question dans une précédente décision :

> "*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)."[1] La condition est toutefois que le plaignant justifie d'un intérêt suffisant.

32. Le plaignant a indiqué dans le formulaire de plainte qu'il cherchait sur le site Internet les données de son médecin traitant et qu'il a ensuite remarqué qu'une connexion non sécurisée était utilisée aussi bien pour le site Internet que pour les formulaires de contact. Toutefois, il n'a pas été établi que des données du plaignant avaient été traitées.

33. De surcroît, la Chambre Contentieuse attire l'attention à cet égard sur un arrêt récent de la Cour de cassation. Dans cet arrêt, la Cour a établi que chaque personne concernée qui estime qu'il est question d'une violation de ses droits en vertu du RGPD peut déposer une plainte auprès de l'autorité de contrôle. Cependant, des personnes concernées dont des données à caractère personnel n'ont pas été traitées peuvent également introduire une plainte dans certains cas. La condition à cela est toutefois que cette personne concernée n'ait pas pu obtenir un avantage déterminé ou un service déterminé parce qu'en raison de l'existence de la pratique constituant une violation telle que présumée, elle a refusé son consentement au traitement[2]. En l'espèce, selon la Chambre Contentieuse, on ne peut pas affirmer qu'il ait été question de ne pas pouvoir utiliser un service, dès lors qu'il existait également d'autres options telle que le contact téléphonique ou la possibilité de compléter les formulaires sur place.

34. Le plaignant ne s'étant pas présenté à l'audition, la Chambre Contentieuse n'a pas pu obtenir de plus amples explications de sa part. Sur la base de la description de la plainte par le plaignant et des pièces déposées, la Chambre Contentieuse doit constater que le plaignant, au moment de l'introduction de la plainte, poursuivait un intérêt public général, à savoir la protection des droits en matière de vie privée de toute personne qui visite le site Internet du défendeur et utilise éventuellement les formulaires de contact sur le site Internet. Le plaignant n'a pas démontré qu'il disposait d'un quelconque intérêt personnel. Dans les circonstances données dans lesquelles il n'est pas apparu que les données à caractère personnel du plaignant avaient été traitées via le formulaire de contact ou qu'il avait l'intention d'utiliser ce formulaire de contact, le fait qu'il était patient de l'hôpital en question n'est pas suffisant pour établir cet intérêt.

---

[1] Décision 80/2020 du 17 décembre 2020 de la Chambre Contentieuse. Voir également la décision 30/2020 de la Chambre contentieuse.
[2] Arrêt de la Cour de cassation c.20.0323.N/1 du 7 octobre 2021.

35. Après examen de la plainte dans le cadre de la procédure sur le fond, il s'est donc avéré que la plainte ne répondait pas aux conditions de recevabilité. La Chambre Contentieuse constate par conséquent que la plainte est et était non recevable en raison de l'absence d'intérêt personnel. Dès lors, la Chambre Contentieuse ne retiendra pas la plainte ni les constatations que le Service d'Inspection a formulées par la suite dans le cadre et en dehors de la plainte pour imposer des sanctions administratives. La Chambre Contentieuse décide donc de procéder à un classement sans suite pour motif technique[3].

III. Considérations générales

Mesures techniques et organisationnelles

36. Il n'empêche que le rapport d'inspection a révélé plusieurs manquements dans la manière dont le défendeur traite les données. À l'aide des constatations formulées dans le rapport d'inspection, la Chambre Contentieuse souhaite formuler plusieurs considérations concernant la prise de mesures de sécurité suffisantes afin de garantir un traitement sûr de données à caractère personnel. La Chambre Contentieuse exécute ainsi la mission générale de l'Autorité de protection des données qui consiste à contribuer à un niveau élevé de protection des données.

37. L'article 24, paragraphe 1 du RGPD dispose ce qui suit : *"Compte tenu de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques, le responsable du traitement met en œuvre des mesures techniques et organisationnelles appropriées pour s'assurer et être en mesure de démontrer que le traitement est effectué conformément au présent règlement. Ces mesures sont réexaminées et actualisées si nécessaire.*"

38. L'article 32du RGPD dispose ce qui suit : "*1. Compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques, le responsable du traitement et le sous-traitant mettent en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque, y compris entre autres, selon les besoins : a) la pseudonymisation et le chiffrement des données à caractère personnel ; b) des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement ; c) des moyens permettant de*

[3] Politique de classement sans suite du 18 juin 2021, rubrique 3.1.A.5.

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

2. Lors de l'évaluation du niveau de sécurité approprié, il doit être tenu compte en particulier des risques que présente le traitement, résultant notamment de la destruction, de la perte, de l'altération, de la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou de l'accès non autorisé à de telles données, de manière accidentelle ou illicite.

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

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

39. Selon l'article 9 du RGPD, les données de santé font partie des données à caractère personnel particulières. Le considérant 51 du RGPD définit ces données comme étant : "*Les données à caractère personnel qui sont, par nature, particulièrement sensibles du point de vue des libertés et des droits fondamentaux méritent une protection spécifique, car le contexte dans lequel elles sont traitées pourrait engendrer des risques importants pour ces libertés et droits.*" Dès lors, le traitement de données de santé doit s'accompagner des plus grandes précautions et toutes les mesures techniques et organisationnelles possibles doivent être prises pour protéger ces données. La principale tâche d'un hôpital est de prodiguer des soins médicaux. Par conséquent, il n'est pas invraisemblable que des patients utilisent ces formulaires de contact pour partager avec l'hôpital des données concernant leur état de santé. En outre, le formulaire pour le service de médiation sert généralement à formuler des insatisfactions et des plaintes, principalement concernant un traitement à l'hôpital et qui sont indirectement liées à ce traitement médical, ce qui implique que des données de santé sont souvent communiquées.

40. Comme cela ressort des articles précités, le responsable du traitement est obligé de mettre en œuvre les mesures techniques et organisationnelles nécessaires afin de garantir

que le traitement de données s'effectue conformément au RGPD. Les hôpitaux dont la tâche principale consiste à prodiguer des soins médicaux traitent régulièrement de grandes quantités de données de santé. Ils doivent donc être particulièrement vigilants et veiller à ce que ces données soient traitées conformément au RGPD. La Chambre Contentieuse souligne que les données à caractère personnel relatives à la santé (et la transmission de celles-ci) doivent être suffisamment sécurisées et que les données doivent dès lors être envoyées sous une forme présentant un niveau de cryptage suffisamment élevé au départ de l'ordinateur de l'utilisateur vers le serveur qui propose un site Internet avec un formulaire. Cela peut se faire en utilisant un certificat de sécurité.

41. Dans le cadre de ce qui précède, le considérant 83 du RGPD précise : "*Afin de garantir la sécurité et de prévenir tout traitement effectué en violation du présent règlement, il importe que le responsable du traitement ou le sous-traitant évalue les risques inhérents au traitement et mette en œuvre des mesures pour les atténuer, telles que le chiffrement. Ces mesures devraient assurer un niveau de sécurité approprié, y compris la confidentialité, compte tenu de l'état des connaissances et des coûts de mise en œuvre par rapport aux risques et à la nature des données à caractère personnel à protéger. Dans le cadre de l'évaluation des risques pour la sécurité des données, il convient de prendre en compte les risques que présente le traitement de données à caractère personnel, tels que la destruction, la perte ou l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière ou l'accès non autorisé à de telles données, de manière accidentelle ou illicite, qui sont susceptibles d'entraîner des dommages physiques, matériels ou un préjudice moral.*"

Émission d'un rapport par le délégué à la protection des données

42. Les lignes directrices concernant les délégués à la protection des données du Groupe 29 donnent les explications suivantes concernant l'émission d'un rapport au niveau le plus élevé de la direction tel que visé à l'article 38, paragraphe 3 du RGPD : "*Si le responsable du traitement ou le sous-traitant prend des décisions qui sont incompatibles avec le RGPD et l'avis du DPD, ce dernier devrait avoir la possibilité d'indiquer clairement son avis divergent au niveau le plus élevé de la direction et aux décideurs. Une telle reddition de compte directe garantit que l'encadrement supérieur (par ex., le conseil d'administration) a connaissance des avis et recommandations du DPD qui s'inscrivent dans le cadre de la mission de ce dernier consistant à informer et à conseiller le responsable du traitement ou le sous-traitant. À cet égard, l'article 38, paragraphe 3, dispose que le DPD "fait directement rapport au niveau le plus élevé de la direction du responsable du traitement ou du sous-traitant*". *Une telle reddition de compte directe garantit que l'encadrement*

supérieur (par ex., le conseil d'administration) a connaissance des avis et recommandations du DPD qui s'inscrivent dans le cadre de la mission de ce dernier consistant à informer et à conseiller le responsable du traitement ou le sous-traitant."[4] Il ressort dès lors du texte cité ci-dessus que le délégué à la protection des données doit pouvoir faire directement rapport au niveau le plus élevé de la direction. La Chambre Contentieuse n'exclut pas qu'il puisse s'agir du directeur général au sein d'un hôpital.

43. La Chambre Contentieuse rappelle que la responsabilité telle qu'exposée à l'article 5.2 du RGPD implique que le responsable du traitement est en mesure de démontrer qu'il répond aux obligations telles que définies dans le RGPD.

IV. Publication de la décision

44. 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 plainte sans suite , en vertu de l'article 100, § 1er, 1° de la LCA**.**

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

[4] Lignes directrices du Groupe 29 *concernant les délégués à la protection des données (DPD)* – WP 243 rev.01, p. 18 (https://ec.europa.eu/newsroom/article29/items/612048/en).