Autorité de protection des données
Gegevensbeschermingsautoriteit

Chambre Contentieuse

Décision quant au fond 127/2022 du 19 août 2022

Numéro de dossier : DOS-2019-05244

Objet : plainte contre un laboratoire d'analyses médicales pour violation des principes de d'intégrité et confidentialité et de transparence

La Chambre Contentieuse de l'Autorité de protection des données, constituée de monsieur Hielke Hijmans, président, et de messieurs Christophe Boeraeve 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 "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 : X, ci-après "le plaignant"

La défenderesse : Laboratoire d'analyses médicales, représentée par Sébastien Popijn, ci-après : "la défenderesse"

I. Faits et procédure

1. Le 4 octobre 2019, le plaignant a introduit une plainte auprès de l'Autorité de protection des données contre la défenderesse.

2. Le plaignant soupçonne le laboratoire d'analyses médicales (ci-après : Laboratoire d'analyses médicales) de ne pas avoir réalisé d'analyse d'impact relative à la protection des données, de ne pas informer les personnes correctement et de traiter des catégories particulières de données, en l'occurrence des données concernant la santé, via un site internet non sécurisé.

   Le plaignant déclare qu'il a eu affaire à plusieurs reprises au laboratoire d'analyses médicales dans le cadre d'analyses médicales. Il a été informé que son médecin a accès aux résultats de ses analyses par voie électronique. Or il s'aperçoit que le site du Laboratoire d'analyses médicales comporte une page d'accès aux données d'analyses médicales intitulée « Cyberlab » dans un protocole http non sécurisé.

3. Le 29 octobre 2019, la plainte est déclarée recevable par le Service de Première Ligne sur la base des articles 58 et 60 de la LCA et la plainte est transmise à la Chambre Contentieuse en vertu de l'article 62, § 1er de la LCA.

4. Le 27 novembre 2019 la Chambre Contentieuse décide de demander une enquête au Service d'Inspection, en vertu des articles 63, 2° et 94, 1° de la LCA.

5. Le 29 novembre 2019, conformément à l'article 96, § 1er de 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.

6. Le 8 septembre 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 comporte des constatations relatives à l'objet de la plainte et effectue les constats suivants :

   1. La partie défenderesse peut être considérée comme responsable de traitement
   2. Sécurisation insuffisante de données de santé en violation des articles 5.1.f), 24, 25 et 32 du RGPD.
   3. Absence d'analyse d'impact relative à la protection des données en violation des articles 35.1 et 35.3 du RGPD).
   4. Manque d'information concernant le traitement des données en violation des articles 12 à 14 du RGPD.

7. Le 21 septembre 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. Le 21 septembre 2021, les parties concernées sont informées par envoi recommandé 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.

   La date limite pour la réception des conclusions en réponse de la défenderesse a été fixée au 2 novembre 2021, celle pour les conclusions en réplique du plaignant au 23 novembre 2021 et enfin celle pour les conclusions en réplique de la défenderesse au 14 décembre 2021.

9. Le 27 septembre 2021, la défenderesse demande une copie du dossier (art. 95, §2, 3° LCA), laquelle lui est transmise le 6 octobre 2021.

10. Le 2 novembre 2021, la Chambre Contentieuse reçoit les conclusions en réponse de la défenderesse.

11. Le 7 novembre 2021, la Chambre Contentieuse reçoit les conclusions en réplique du plaignant.

12. Le 9 décembre 2021, la Chambre Contentieuse reçoit les conclusions en réplique de la part de la défenderesse.

13. Le 25 juillet 2022, la Chambre Contentieuse fait connaître à la défenderesse son intention de procéder à l'imposition d'une amende administrative ainsi que le montant de celle-ci, afin de donner à la défenderesse l'occasion de se défendre avant que la sanction soit effectivement infligée.

14. Le 15 août 2022, la Chambre Contentieuse reçoit la réaction de la défenderesse concernant l'intention d'infliger une amende administrative et le montant de celle-ci.

II. Motivation

II.1. La responsabilité du traitement

15. Dans son rapport d'enquête, le Service d'inspection (ci-après: SI) détermine que la partie défenderesse peut être qualifiée de responsable de traitement. Cette position est initialement contestée par la partie défenderesse, mais finalement accepté dans ses conclusions de synthèse, suite aux conclusions en réplique du plaignant.

16. La Chambre contentieuse décide que la partie défenderesse peut être qualifiée de responsable de traitement étant donné qu'elle détermine les finalités et les moyens du traitement.

17. Elle rappelle néanmoins qu'en vertu du principe de responsabilité de l'article 24 du RGPD, la défenderesse doit elle-même être en mesure d'établir ses responsabilités et ses obligations sur base du RGPD. La Chambre contentieuse ajoute par ailleurs que les changements de position de la défenderesse au cours de la procédure apportent une évidente confusion dans sa défense, puisqu' originellement elle avance par exemple qu'elle n'est pas soumise à l'obligation de réaliser une AIPD parce qu'elle n'est que sous-traitante[1] (et que les sous-traitant n'ont pas d'obligation de réaliser d'AIPD) pour ensuite indiquer que l'absence de réalisation d'une AIPD est due au fait que, originellement, les traitements ne remplissaient pas les critères l'obligeant à en réaliser une. [2] Ces positions son bien évidemment incompatibles entre-elles.

II.2. Intérêt du plaignant.

18. Il ressort du dossier que le médecin du plaignant a fait effectuer par la défenderesse plusieurs analyses médicales pour son patient. La défenderesse traite donc ou a traité des données à caractère personnel du plaignant. Ce dernier dispose donc d'un intérêt à agir dans ce dossier.

II.3. Constatation 1 : sécurisation insuffisante de données de santé (articles 5.1.f), 24, 25 et 32 du RGPD)

19. Il ressort du rapport d'enquête que la défenderesse dispose d'un site web. La page d'accueil de ce site web renseigne une autre page du laboratoire d'analyses médicales sous un intitulé « Consulter les résultats », qui renvoie vers le « Cyberlab », le serveur de résultat en ligne de la défenderesse qui permet aux médecins d'accéder en temps réel aux résultats et historiques des analyses de leurs patients.

20. Le SI a pu constater lors de son premier rapport d'enquête technologique du 14 janvier 2021 (ci-après : le premier rapport technologique) que ce site internet ne contient pas de chiffrement (l'identifiant et le mot de passe collectés sont transmis non chiffrés), étant donné qu'il utilise un protocole « http » au lieu d'un protocole crypté « https ».

[1] Conclusions de la défenderesse, p. 9.

[2] Conclusion de synthèse de la défenderesse, p. 7.

21. Le SI constate à cette occasion que « Le site d'accès au Cyberlab est donc non sécurisé et est sensible par attaque de type "homme au milieu" (Man in the middle). L'identifiant et le mot de passe collectés sont transmis non chiffrés […]».

22. Suite aux réponses fournies par la défenderesse au cours de l'enquête, un rapport de suivi du rapport d'enquête technologique est produit le 6 juillet 2021 (ci-après, le rapport de suivi). Ce rapport établit notamment que depuis l'établissement du premier rapport technologique, le « Cyberlab » « a été sécurisé puisqu'accessible au moyen du protocole https en lieu et place du protocole http. L'utilisation de ce protocole sécurisé empêche la divulgation des informations de connexion et donc d'accès aux résultats d'analyses des patients par des attaques de type « homme au milieu » (Man in the Middle). »

23. Le second rapport ajoute que « le protocole d'encryption est TLS 1.2 pour lequel plusieurs vulnérabilités existent » et que « par rapport au rapport initial, l'on peut remarquer des progrès [en ce qui concerne] la sécurisation des informations en transit puisque l'implémentation du protocole TLS 1.2 a été réalisée en lieu et place d'une simple connexion http. ».

24. Sur base de ces deux rapports technologiques, le SI conclut à une violation des articles 5.1.f), 24, 25 et 32 du RGPD.

25. Les arguments de la partie défenderesse sont résumés de la façon suivante :

    - le grief retenu à son encontre n'est plus d'actualité, comme constaté par le SI et reconnu par le plaignant dans ses conclusions ;

    - avant la mise en place du chiffrement, le site n'était pas dépourvu de mesures de sécurité, puisque le médecin souhaitant y accéder doit disposer d'un identifiant et d'un code secret personnel ;

    - une attaque du type « Man in the Middle » suppose que le pirate ait préalablement pris le contrôle de l'infrastructure informatique du médecin. Auquel cas il n'aurait de toute façon accès qu'aux résultats de l'analyse d'un patient ;

    - Aucune attaque de ce type n'a été détecté et l'éditeur du logiciel Cyberlab ne semble pas imposer l'installation d'un certificat https ;

    - la formulation «garantir une sécurité appropriée » de l'article 5.1.f) du RGPD » suppose de regarder l'environnement existant et pas de raisonner *in abstracto* ;

    - la défenderesse a pris la décision de renforcer la sécurité de l'accès aux données en mettant en place un système de « double identification des médecins »[3], qui nécessitera leur consultation préalable.

[3] Terminologie utilisée par la partie défenderesse.

26. Sur base du rapport d'enquête et des arguments des parties, la Chambre contentieuse constate que le site web du Cyberlab de la partie défenderesse était non-sécurisé au moment de la plainte et du lancement de l'enquête. Suite à la prise de contact du SI avec la défenderesse, le site a été sécurisé via la mise en œuvre du protocole TLS 1.2, à une date indéterminée située entre le premier rapport technologique du 14 janvier 2021 et le second rapport technologique du 6 juillet 2021.

27. Au-delà des considérations et arguments soulevés par la partie défenderesse, le protocole TLS est un protocole de chiffrement de base qui existe depuis 1999. Toute entité qui vise à assurer une sécurité standard des données transitant par son site web en fait ou devrait en faire usage. Il s'agit d'un standard qui est très largement recommandé[4].

28. Ceci est d'autant plus valable pour une plateforme qui traite et permet d'accéder à des résultats d'analyses médicales de centaines ou de milliers de patients[5]. Ce standard – et plus spécifiquement sa version TLS 1.2 - n'a été mise en place qu'après que le SI ait pris contact avec la défenderesse.

29. Le principe d'intégrité et de confidentialité, inscrit à l'article 5.1.f) du RGPD est rédigé comme suit :

    « Les données à caractère personnel doivent être traitées de façon à garantir une sécurité appropriée des données à caractère personnel, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées (intégrité et confidentialité) »

    Il est plus amplement développé à l'article 32 du RGPD.

30. En l'espèce, la Chambre contentieuse décide qu'une page web permettant aux médecins de consulter à distance les résultats d'analyses médicales de patients sans offrir de chiffrement, **viole le principe d'intégrité et de confidentialité inscrit aux articles 5.1.f) à l'article 32 du RGPD**.

31. Au-delà de ces articles, le SI estime également qu'en tant que laboratoire d'analyses médicales, la défenderesse traite quotidiennement des données de santé. Il était de sa responsabilité de mettre en œuvre des mesures techniques et organisationnelles appropriées et d'assurer la protection des données dès la conception et par défaut, conformément aux articles 24 et 25 du RGPD et conclut donc à une violation de ces articles.

---

[4] Voir par exemple les recommandations de la CNIL sur la sécurisation des sites webs ; les lignes directrices de l'EDPS concernant la protection des données personnelles traitées par services web fournis par les institutions de l'UE (point 82).

[5] La partie défenderesse déclarant dans ses conclusions qu'elle traitait 50 analyses par jour avant le début de la pandémie du COVID et que ce chiffre a largement augmenté depuis.

32. La défenderesse se défend sur la constatation numéro 1 dans son ensemble avec les arguments résumés au point 25 et ne fait pas de distinction entre la violation des articles 5.1.f) et 32 d'une part et les articles 24 et 25 d'autre part.

33. La Chambre contentieuse estime que le constat de violation des articles 5.1.f) et 32 du RGPD est suffisant pour sanctionner le manquement relatif à la sécurité du traitement.

34. Par ailleurs, dans ces conclusions de synthèse, la partie défenderesse indique « qu'en vue de renforcer encore la sécurité d'accès aux données, le laboratoire d'analyses médicales a pris la décision de mettre en place un système de double identification des médecins ». La Chambre contentieuse comprend de cette phrase que la partie défenderesse se réfère à un système d'authentification multifactoriel. En l'espèce, la Chambre contentieuse souligne l'importance de mettre en place un système d'authentification forte, qui pourrait être bifactorielle. Elle ajoute, bien que cet aspect ne fasse pas partie des constatations du SI, que l'absence de système d'authentification forte pourrait poser question quant au respect du principe de confidentialité et d'intégrité prévu aux articles 5.1.f) et 32 du RGPD.

II.4. Constatation 2 : absence d'analyse d'impact relative à la protection des données (articles 35.1 et 35.3 du RGPD).

35. Pour le Service d'Inspection, la défenderesse a violé les articles 35.1 et 35.3 du RGPD en ne réalisant pas d'Analyse d'impact de la protection des données, alors qu'elle traite à grande échelle des données de santé.

36. La partie défenderesse conteste le fait qu'elle traitait à l'époque des données à grande échelle, indiquant qu'elle ne traitait qu'une cinquantaine d'analyses par jour. Elle estime que la notion de « grande échelle » inclue à l'article 35.3.b) n'est pas suffisamment objective. Elle s'appuie également sur des informations présentes sur le site web de la CNIL qui indiquent que les laboratoires d'analyses médicales doivent vérifier, en fonction de leur projet, s'il est nécessaire d'effectuer une analyse d'impact sur la protection des données, ce qui pour la défenderesse indique que cette obligation n'est pas systématique[6].

37. Elle ajoute que le nombre d'analyses traitées par le laboratoire d'analyses médicales a considérablement augmenté en raison de la pandémie Covid-19. Par conséquent, elle estime aujourd'hui entrer dans les conditions d'un traitement de données de santé à grande échelle et a donc fait réaliser une AIPD

38. Le plaignant estime pour sa part que les traitements sont bien des traitements de données de santé opérés à grande échelle. Il estime en effet que ceux-ci tombent sous le point 5 de

[6] https://www.cnil.fr/fr/cnil-direct/question/laboratoire-danalyse-de-biologie-medicale-que-faire

la Décision du Secrétariat Général de l'APD n°01/2019 du 16 janvier 2019[7] qui est formulé comme suit :

« *Lorsque des catégories particulières de données à caractère personnel au sens de l'article 9 du RGPD* [...] *sont échangées systématiquement entre plusieurs responsables du traitement.* ».

39. Le plaignant considère également que même si les traitements ne tombent pas sous ce point, ils constituent toujours des traitements de données de santé opérés à grande échelle. Le plaignant conteste que la définition de grande échelle soit laissée entièrement à l'appréciation de l'autorité de contrôle, puisque elle est balisée par le considérant 91 du RGPD et les lignes directrices du Groupe de travail "Article 29" (G29) sur les délégués à la protection des données[8].

40. La question portée à l'examen de la Chambre contentieuse est de savoir si la défenderesse était soumise à l'obligation de réaliser à une AIPD sur base des articles 35.1 et 35.3 du RGPD avant que la plainte ne soit introduite, en raison du fait que les traitements de données qu'elle effectue constituent des traitements de données à grande échelle.

41. La Chambre contentieuse note en premier lieu qu'il n'est pas contesté que la défenderesse traite des données de santé au sens de l'article 9.1 du RGPD. L'examen de la Chambre contentieuse se porte donc sur la notion de « grande échelle ».

42. La Chambre contentieuse note que la défenderesse critique la notion de « grande échelle » en la qualifiant d'imprécise.

43. La Chambre contentieuse convient que la notion de « grande échelle » est sujette à appréciation, mais elle conteste que celle-ci soit source d'incertitude juridique. En effet, aussi bien le RGPD[9], que des recommandations nationales et européennes permettent de clarifier les critères qui déclenchent une obligation de réaliser une AIPD. Celles-ci sont reprises dans le Guide Analyse d'impact relative à la protection des données publié par l'APD sur son site web[10] et qui contient quatre critères provenant des lignes directrices européennes permettant de déterminer si un traitement est effectué à grande échelle[11]. Il s'agit des critères suivants :

    - le nombre de personnes concernées, soit en valeur absolue, soit en proportion de la population considérée;

---

[7] Disponible sur : https://www.autoriteprotectiondonnees.be/publications/decision-n-01-2019-du-16-janvier-2019.pdf

[8] Disponible sur : https://ec.europa.eu/newsroom/article29/items/612048

[9] RGPD, considérant 91.

[10] Autorité de protection des données, « Guide Analyse d'impact relative à la protection des données », version 4.0 du 21 avril 2021, p. 2-7. (Disponible sur : https://www.autoriteprotectiondonnees.be/publications/guide-analyse-d-impact-relative-a-la-protection-des-donnees.pdf)

[11] *Ibidem*, p. 6.

- le volume de données et/ou l'éventail des différents éléments de données traitées;
- la durée ou la permanence de l'activité de traitement de données;
- l'étendue géographique de l'activité de traitement.

44. La Chambre contentieuse fait par ailleurs remarquer à la défenderesse qu'elle contribue elle-même à entretenir une certaine subjectivité de cette notion en se référant dans ses conclusions à des éléments vagues en considérant « qu'à l'origine » ses activités ne constituaient pas un traitement à grande échelle, mais que « les analyses traitées par le laboratoire d'analyses médicales ayant considérablement augmentées en raison de la pandémie Covid-19 », elle estime qu'elle effectue dorénavant des traitements à grande échelle. La défenderesse aurait dû, sur base du principe de responsabilité de l'article 24, clarifier son interprétation de la notion de « grande échelle » en indiquant les critères objectifs sur lesquels elle se base pour estimer que ses activités ont fini par entrer dans la catégorie de traitements à grande échelle, alors que selon elle, elles ne remplissaient pas ce critère au départ.

45. En l'espèce, plusieurs éléments permettent à la Chambre contentieuse de conclure que la défenderesse était bien soumise à une AIPD avant qu'elle ne décide de la réaliser.

46. Tout d'abord, la Chambre contentieuse ne dispose d'aucune information indiquant que l'étendue des traitements de données opérés par la partie défenderesse aurait radicalement évolué en raison de la pandémie COVID-19 jusqu'à devenir un traitement à grande échelle. La défenderesse avance en effet qu'avant la pandémie du COVID-19, le laboratoire réalisait une cinquantaine d'analyses par jour, sans préciser le nombre d'analyses réalisées actuellement ou durant la pandémie.

47. De plus, le document de l'AIPD réalisé par un prestataire externe[12] avance quant à lui la conclusion suivante : « Le traitement de données décrit doit être considéré comme susceptible d'entraîner un risque élevé pour les droits et libertés des personnes physiques. En effet, l'analyse des prélèvements ainsi que le rendu des résultats d'analyses traitent des catégories particulières de données à caractère personnel à grande échelle. Une AIPD doit être effectuée par le laboratoire d'analyses médicales. »

48. La Chambre Contentieuse conclut donc que les traitements au moment de la plainte et du rapport d'enquête sont des traitements à grande échelle.

[12] Document fourni à la Chambre Contentieuse sur proposition de la partie défenderesse suite à l'échange de conclusions. Ce document n'avait pas encore été rédigé lors de l'enquête du Service d'inspection.

49. Surabondamment, la Chambre contentieuse est d'avis que les traitements en question tombent sous la définition du point 5 de la Décision du Secrétariat Général n°01/2019 du 16 janvier 2019 qui est formulé comme suit :

    « Lorsque des catégories particulières de données à caractère personnel au sens de l'article 9 du RGPD [...] sont échangées systématiquement entre plusieurs responsables du traitement. ».

    Il est en effet établit que la défenderesse effectue des analyses pour de nombreux médecins, eux-mêmes considérés comme responsables du traitement, qui peuvent par la suite consulter les résultats des analyses. Pour la Chambre contentieuse, la réalisation d'une AIPD aurait donc également pu être obligatoire sur cette base.

    Enfin, la Chambre Contentieuse rappelle qu'en vertu de l'article 35.1 du RGPD, une analyse d'impact doit être réalisée **avant** que le traitement envisagé ne soit effectué[13].

50. Sur base des éléments ci-dessus, la Chambre Contentieuse conclut que la défenderesse aurait déjà dû avoir réalisé une AIPD avant que la plainte ne soit introduite, et qu'en ne l'ayant pas réalisée, la défenderesse a violé les articles 35.1 et 35.3 du RGPD.

II.5. Constatation 3 : manque d'information concernant le traitement des données (articles 12 à 14 du RGPD)

51. Il ressort du rapport d'enquête technologique du 14 janvier 2021 qu'aucune politique de vie privée n'était disponible sur le site web de laboratoire d'analyses médicales à cette date.

52. Selon son conseiller juridique, le laboratoire d'analyses médicales aurait prévu un affichage des informations RGPD dans ses propres centres de prélèvements. Cela étant, il reconnait que cela ne représente qu'une petite partie des patients pour lesquels le laboratoire d'analyses médicales est chargée de procéder à des analyses.

53. Le rapport du 6 juillet 2021 de suivi du rapport d'enquête technologique a montré qu'une politique de vie privée figurait à présent sur le site web de laboratoire d'analyses médicales.

54. Le Service d'inspection conclut à une violation de l'obligation de fournir de l'information prévu aux articles 12 à 14 du RGPD étant donné qu'aucune politique de vie privée n'était présente sur le site web au moment du premier rapport technologique.

55. Dans un premier temps, la défenderesse conteste cette violation en indiquant qu'elle se considérait alors comme sous-traitant. La défenderesse ayant finalement reconnu être

[13] C'est la Chambre contentieuse qui souligne.

responsable de traitement dans ses conclusions de synthèse, elle fait valoir que depuis le mois de mars 2021, une politique de vie privée est bien présente sur le site.

56. Elle souligne également que le RGPD n'impose pas que cette information soit publiée sur le site web. Elle considère également qu'au vu du faible nombre de traitements opérés avant le COVID, un affichage dans ses centres de prélèvement était suffisant. Elle ajoute que l'évolution soudaine de ses activités depuis la pandémie justifie qu'elle affiche cette information sur son site web.

57. La Chambre contentieuse constate tout d'abord que la défenderesse n'apporte pas la preuve du fait que la politique de confidentialité se trouvait affichée dans ses centres de prélèvement. Elle estime également que le site web de la défenderesse ne peut être considéré comme une simple vitrine commerciale comme le soutient la défenderesse dans ses conclusions. En effet, ce site web contient un lien vers le site web du Cyberlab qui permet la consultation des résultats d'analyse. Ce dernier site web ne contenait pas non plus de politique de confidentialité. Les deux sites web constituent donc un outil opérationnel important pour les activités de la défenderesse et non pas une simple vitrine commerciale.

58. Le G29 dans ses lignes directrices sur la transparence indique notamment que « Chaque entreprise disposant d'un site internet devrait publier une déclaration ou un avis sur la protection de la vie privée sur son site. Un lien direct vers cette déclaration ou cet avis sur la protection de la vie privée devrait être clairement visible sur chaque page de ce site internet sous un terme communément utilisé (comme «Confidentialité», «Politique de confidentialité» ou «Avis de protection de la vie privée»).» [14] Par ailleurs, il indique que « l'intégralité des informations adressées à une personne concernée devrait également être accessible à un endroit unique ou dans un même document (au format papier ou électronique) pouvant être aisément consulté par cette personne si elle souhaite consulter l'intégralité des informations qui lui sont adressées. »[15].

59. Sur base des éléments ci-dessus, la Chambre contentieuse décide, qu'en ne publiant pas sa politique de confidentialité sur son site internet, la défenderesse a **violé les articles 12, 13 et 14 du RGPD**.

60. Elle note qu'à l'heure actuelle, une politique de confidentialité est bien présente sur le site web de la défenderesse.

[14] Groupe de travail «Article 29», « Lignes directrices sur la transparence au sens du règlement (UE) 2016/679 », version révisée et adoptée le 11 avril 2018 (Disponible sur : https://ec.europa.eu/newsroom/article29/items/622227), point 11.

[15] *Ibidem*, point 17.

II.6. Sanction

61. La Chambre Contentieuse décide d'infliger une amende administrative. Comme cela ressort clairement du considérant 148, le RGPD prévoit en effet que des sanctions, y compris des amendes administratives, soient infligées pour *toute* violation sérieuse - donc y compris à la première constatation d'une violation -, en complément ou à la place des mesures appropriées qui sont imposées.[16] La Chambre Contentieuse démontre ci-après que les violations des articles 5.1.f), 12, 13, 14 et 32 et 35.1 et 35.3 du RGPD commises par la défenderesse ne sont en aucun cas des violations mineures et que l'amende ne constituerait pas une charge disproportionnée à une personne physique au sens du considérant 148 du RGPD, deux cas qui permettraient de renoncer à une amende. Le fait qu'il s'agisse d'une première constatation d'une violation du RGPD commise par la défenderesse n'affecte en rien la possibilité pour la Chambre Contentieuse d'infliger une amende administrative. La Chambre Contentieuse inflige une amende administrative en application de l'article 58.2 i) du RGPD. L'instrument de l'amende administrative n'a nullement pour but de mettre fin mettre fin à une infraction commise mais bien de faire appliquer efficacement les règles du RGPD. Pour mettre fin à une infraction, le RGPD et la LCA prévoient plusieurs mesures correctrices, dont les ordres cités à l'article 100, § 1er, 8° et 9° de la LCA.

62. Vu l'article 83 du RGPD et la jurisprudence[17] de la Cour des marchés, la Chambre Contentieuse motive l'imposition d'une sanction administrative de *manière concrète*:

    La Chambre contentieuse retient les circonstances aggravantes ci-dessous :

    - Le fait que les données traitées soient des données de santé et qu'elles le soient à grande échelle (article 83.2.g) du RGPD);
    - Le manque de cohérence dans les explications de la défenderesse qui n'était pas à même de déterminer si elle était responsable de traitement ou sous-traitant[18] et n'a par conséquent pas correctement remplit les obligation qui découlent du RGPD, comme le démontrent les constats de violation (article 83.2.k) du RGPD);

---

[16] Le considérant 148 dispose ce qui suit : "Afin de renforcer l'application des règles du présent règlement, des sanctions y compris des amendes administratives devraient être infligées pour toute violation du présent règlement, en complément ou à la place des mesures appropriées imposées par l'autorité de contrôle en vertu du présent règlement. En cas de violation mineure ou si l'amende susceptible d'être imposée constitue une charge disproportionnée pour une personne physique, un rappel à l'ordre peut être adressé plutôt qu'une amende. Il convient toutefois de tenir dûment compte de la nature, de la gravité et de la durée de la violation, du caractère de la violation et des mesures prises pour atténuer le dommage subi, du degré de responsabilité ou de toute violation pertinente commise précédemment, de la manière dont l'autorité de contrôle a eu connaissance de la violation, du respect des mesures ordonnées à l'encontre du responsable du traitement ou du sous-traitant, de l'application d'un code de conduite, et de toute autre circonstance aggravante ou atténuante. L'application de sanctions y compris d'amendes administratives devrait faire l'objet de garanties procédurales appropriées conformément aux principes généraux du droit de l'Union et de la Charte, y compris le droit à une protection juridictionnelle effective et à une procédure régulière. [soulignement propre]

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

[18] Voir point 17 ci-dessus.

- Les violations constatées, bien qu'elles n'apparaissent pas délibérées, démontrent une importante négligence dans le respect de la législation relative à la protection des données (article 83.2.b) du RGPD) ;
- Cet aspect est renforcé par le fait que ce n'est qu'après l'intervention du SI que de nombreuses actions de mises en conformité ont été entreprises (article 83.2.a) du RGPD).

La Chambre contentieuse retient les circonstances atténuantes ci-dessous :

- Le fait que la défenderesse n'a pas fait l'objet de violations constatées par le Chambre contentieuse par le passé (article 83.2.e) du RGPD) ;
- La défenderesse a remédié aux lacunes constatées avant que la Chambre contentieuse ne rende sa décision (article 83.2.f) du RGPD).

63. Le 25 juillet 2022, la Chambre Contentieuse fait connaître à la défenderesse son intention de procéder à l'imposition d'une amende administrative de 25.000 EUR. Le 15 août 2022, la Chambre Contentieuse reçoit la réaction de la défenderesse concernant l'intention d'infliger une amende administrative et le montant de celle-ci. La défenderesse fait valoir les éléments suivants:

    a. ni le demandeur ni aucune autre personne n'a subi un dommage des violations alléguées;

    b. le défendeur a apporté tous les correctifs adéquats et ce sans attendre l'issue de cette procédure;

    c. les violations alléguées ont été commises par négligence;

    d. le défendeur n'a pas précédemment commis de violations;

    e. Le supposé manque de cohérence dans les explications du défendeur ne peut lui être reproché car il est dû à un mauvais conseil et qu'en tout état de cause on ne peut reprocher à une personne la manière dont elle se défend;

    f. L'activité principale consiste à remplir une mission d'intérêt général à savoir contribuer par des analyses biomédicales à la santé public;

    g. Le chiffres d'affaires du défendeur pour l'exercice dont question est certes de (.. EUR) mais qu'il y a lieu de tenir compte de la perte de (..EUR) pour déterminer les moyens financiers du défendeur.

64. A cet égard, la Chambre Contentieuse précise que les arguments **b** et **d** de la défenderesse ont déjà été retenus comme circonstances atténuantes lors de l'envoi du formulaire d'amendes (voir "circonstances atténuantes" au point 62).

65. Pour ce qui concerne l'argument **a**, la Chambre contentieuse rappelle que le droit à la protection des données est un droit fondamental de tout un chacun et est repris en tant que tel à l'article 8 de la Charte des droits fondamentaux de l'Union européenne. Le responsable du traitement n'a aucune compétence d'appréciation quant à l'ampleur de ce droit en fonction du prétendu faible impact de la violation, alors que le RGPD impose des obligation positives. En effet, pour de nombreuses obligations prévues par le RGPD, telles que la nomination d'un DPD, la communication d'informations de manière transparente, la réalisation d'une AIPD etc, l'absence de mise en œuvre occasionnera rarement un dommage direct à une personne concernée Ceci ne dispense pas pour autant les responsables de traitement de leur mise en œuvre, d'autant que le RGPD ne conditionne pas l'imposition d'une amende au responsable de traitement à la réalisation d'un dommage.

La Chambre contentieuse précise que l'argument **c**, de le défenderesse, lié à l'argument **e** ont été retenus par la Chambre contentieuse comme des circonstances aggravantes. En effet, les manquement identifiés démontrent une négligence importante de la part du responsable de traitement par rapport à ses obligations relatives la protection des données. Le caractère important de cette négligence est renforcé par les arguments contradictoires de la défenderesse dans ses conclusions. Bien qu'une défenderesse soit évidemment libre de choisir les arguments qu'elle présente, les explications contradictoires peuvent être révélatrices d'une insuffisante prise en compte de ses responsabilités au regard du RGPD. La Chambre contentieuse a préalablement développé les aspects contradictoires des explications de la défenderesse (point 17).

La Chambre contentieuse juge l'argument **f** non-pertinent en l'espèce. En effet, seules les autorités publiques sont exemptées de la possibilité de se voir imposer une amende, en vertu de l'article 221, §2 de la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel. La défenderesse n'étant pas une autorité publique, cet article ne lui est pas applicable. Par ailleurs, le fait que la défenderesse traite des données de santé à grande échelle devrait l'inciter à agir avec d'autant plus de diligence en ce qui concerne la protection de ces données et constitue à ce titre un facteur aggravant des violations constatées et non une circonstance atténuante.

En ce qui concerne le point **g**, la Chambre contentieuse rappelle que c'est bien le chiffre d'affaire qui est retenu comme critère de détermination du montant maximal des amendes dans le RGPD et non le compte de résultat. Ce choix du législateur européen a été fait à dessein afin d'éviter que les variations dans le compte de résultat ne viennent limiter la capacité des autorités de supervision de données d'imposer des amendes effectives. La Chambre contentieuse est cependant sensible à la situation financière difficile de la défenderesse durant l'année de référence et aux pertes importantes subies, ce qui peut

constituer une circonstance atténuante prévue à l'article 83.2.k) du RGPD. Elle décide par conséquent de diminuer le montant de l'amende à 20.000 EUR.

66. Dans un souci d'exhaustivité, la Chambre contentieuse souhaite renvoyer aux Lignes directrices (Guidelines 04/2022 Guidelines 04/2022 on the calculation of administrative fines under the GDPR), que l'EDPB a publiées sur son site web le 16 mai 2022, pour consultation.

    Ces lignes directrices n'étant pas encore définitives, la Chambre contentieuse a décidé de ne pas en tenir compte pour déterminer le montant de l'amende dans la présente procédure.

67. L'ensemble des éléments exposés ci-dessus justifie une sanction effective, proportionnée et dissuasive, telle que visée à l'article 83 du RGPD, compte tenu des critères d'appréciation qu'il contient. La Chambre Contentieuse souligne également que les autres critères énoncés à l'article 83.2 du RGPD ne sont pas pertinents en l'espèce et n'entrainent donc pas une amende administrative autre que celle déterminée par la Chambre Contentieuse dans le cadre de la présente décision.

68. Conformément à ce qui précède, la Chambre contentieuse constate qu'elle peut se baser sur les chiffres annuels de laboratoire d'analyses médicales pour déterminer le montant de l'amende administrative qu'elle entend imposer à la partie défenderesse.

69. La Chambre contentieuse se réfère aux comptes annuels déposés auprès de la Banque Nationale de Belgique (BNB) le 26 juillet 2021, qui font état d'un chiffre d'affaires pour l'exercice 2020 de (..EUR).

70. L'amende administrative prévue de **20.000,00 euros correspond dans ce cas à 0,07 % du chiffre d'affaires annuel** de la partie défenderesse pour l'année 2020. La Chambre contentieuse se réfère aux comptes annuels déposés auprès de la Banque Nationale de Belgique (BNB) le 26 juillet 2021, qui font état d'un chiffre d'affaires pour l'exercice 2020 de (..EUR).

71. La Chambre contentieuse indique que le montant maximal de l'amende administrative pour une violation est déterminé par les articles 83.4 et 83.4 du RGPD. Le montant de l'amende infligée dans la présente décision est nettement inférieur au montant maximal prévu (qui aurait pu atteindre un maximum de 20.000.000 EUR), étant donné que la Chambre contentieuse a tenu compte de tous les critères pertinents énoncés à l'article 83.2 du RGPD. En outre, la Chambre contentieuse évalue les éléments concrets de chaque cas individuellement afin d'imposer une sanction appropriée.

III. Publication de la décision

72. 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 des articles 100,§1°,13° et 101 de la LCA, **d'imposer une amende de 20.000 EUR pour la violations des articles 5.1.f), 12, 13, 14, 32, 35.1 et 35.3 du RGPD**

- en vertu de l'article 100,§1, 1° de la LCA, de classer le dossier sans suite pour les constats restants.

Conformément à l'article 108, § 1 de la LCA, un recours contre cette décision peut être introduit, dans un délai de trente jours à compter de sa notification, auprès de la Cour des Marchés (cour d'appel de Bruxelles), avec l'Autorité de protection des données comme partie défenderesse.

Un tel recours peut être introduit au moyen d'une requête interlocutoire qui doit contenir les informations énumérées à l'article 1034ter du Code judiciaire[19]. La requête interlocutoire doit être déposée au greffe de la Cour des Marchés conformément à l'article 1034*quinquies* du C. jud.[20], ou via le système d'information e-Deposit du Ministère de la Justice (article 32ter du C. jud.).

(sé). Hielke HIJMANS

Président de la Chambre Contentieuse

---

[19] 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.

[20] 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