



Chambre Contentieuse

Décision quant au fond 64/2025 du 1er avril 2025

Numéro de dossier : DOS-2020-01932

Objet : Plainte relative à une décision de licenciement prise à la suite de la consultation du dossier médical de la plaignante par sa supérieure hiérarchique

La Chambre Contentieuse de l'Autorité de protection des données, constituée de monsieur Hielke HUMANS, 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 2019¹;

Vu les pièces du dossier;

A pris la décision suivante concernant :

La plaignante : X, représentée par Maître Mélissa Fernandez Viesca, ci-après « la plaignante »

La défenderesse : Association Hospitalière Y, ci-après « la défenderesse »

¹ Le nouveau règlement d'ordre intérieur de l'APD, consécutif aux modifications apportées par la Loi du 25 décembre 2023 modifiant la loi du 3 décembre 2017 portant création de l'autorité de protection des données (LCA) est entré en vigueur le 01/06/2024.

Conformément à l'article 56 de la loi du 25 décembre 2023, il est uniquement d'application aux plaintes, dossiers de médiation, requêtes, inspections et procédures devant la Chambre Contentieuse initiés à partir de cette date : <https://www.autoriteprotectiondonnees.be/publications/reglement-d-ordre-interieur-de-l-autorite-de-protection-des-donnees.pdf>.

Les dossiers initiés avant le 01/06/2024 comme en l'espèce sont soumis aux dispositions de la LCA non-modifiée par la Loi du 25 décembre 2023 et du règlement d'ordre intérieur tel qu'il existait avant cette date.

I. Faits et procédure

1. Le 22 avril 2020, la plaignante introduit une plainte auprès de l’Autorité de protection des données contre la défenderesse.
2. L’objet de la plainte concerne une décision de licenciement, laquelle décision se fonderait sur des données de santé relatives à la plaignante qui auraient été consultées d’une manière illicite par la supérieure hiérarchique de celle-ci (ci-après désignée « la supérieure hiérarchique »).
3. La plaignante a travaillé en tant qu’employée au sein de l’établissement de la défenderesse.
4. Le 3 mars 2020, la défenderesse notifie la plaignante de la fin de leur relation de travail.
5. Le 16 avril 2020, la défenderesse, en réponse à une demande de la plaignante, informe cette dernière que son dossier médical a fait l’objet d’une consultation par sa supérieure hiérarchique en date du 2 mars 2020. Selon ce même courrier recommandé, il s’agirait de l’unique consultation opérée par elle. En outre, la défenderesse précise avoir entamé une enquête interne à ce sujet.
6. Dans son formulaire de plainte, la plaignante indique avoir été mise au courant de la fin de son contrat de travail lors d’une réunion dans laquelle il lui aurait été expliqué que l’un des motifs de son licenciement concernait son état de santé pour lequel sa supérieure hiérarchique nourrissait des craintes. Celle-ci souhaitait, selon ses dires, vérifier que son état de santé était approprié afin d’apprendre son licenciement.
7. Le 4 juin 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.
8. Le 7 janvier 2021 la Chambre Contentieuse décide, en vertu de l’article 95, § 1^{er}, 1^o et de l’article 98 de la LCA, que **le dossier peut être traité sur le fond**.
9. À la même date, 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 18 février 2021, celle pour les conclusions en réplique de la plaignante au 11 mars 2021 et celle pour les conclusions en duplique de la défenderesse au 1er avril 2021.
10. Les parties sont invitées à se défendre au regard des griefs suivants retenus par la Chambre Contentieuse :
 - A. **Quant à la base de licéité du traitement de données personnelles reproché (violation potentielle des art. 5.1.a) et 6 du RGPD)**

En tenant compte des éléments de fait soulevés par la plainte, la Chambre contentieuse invite la défenderesse à émettre son point de vue sur les points suivants, et invite la plaignante à y répondre si elle le souhaite, en particulier si elle a des éléments de faits complémentaires à apporter :

- La consultation par la supérieure hiérarchique du dossier médical de la plaignante constitue-t-il un traitement de données à caractère personnel pour lequel la défenderesse est responsable de traitement au sens de l'article 4.7 du RGPD ? A défaut, en quelle qualité a-t-elle consulté le dossier médical de la plaignante ?
- La défenderesse et/ou la supérieure hiérarchique disposaient-elles d'une base de licéité valable pour la consultation du dossier médical de la plaignante conformément à l'article 6 du RGPD ? Ce traitement de données était-il licite et transparent au sens de l'article 5.1.a) du RGPD ?

B. Quant à la qualification des faits sous l'angle de l'article 33 du RGPD

Dans la mesure où les faits relatés (consultation du dossier médical de la plaignante) seraient potentiellement constitutifs d'une violation de données à caractère personnel au sens de l'article 33 du RGPD, la défenderesse – dans la mesure où elle serait responsable de ce traitement de données – a-t-elle effectué une notification de la violation à l'autorité de contrôle conformément à l'article 33.1 RGPD, et a-t-elle documenté les faits, ses effets et les mesures prises pour y remédier le cas échéant conformément à l'article 33.5 du RGPD ? Le cas échéant, quel fut le résultat de l'enquête interne annoncée par la défenderesse dans sa lettre à la plaignante du 16 avril 2020, et quelles mesures ont été prises pour remédier à la violation de données, le cas échéant ?

11. Toujours à la même date, la plaignante et la défenderesse acceptent de recevoir toutes les communications relatives à l'affaire par voie électronique. La plaignante fait remarquer quelques erreurs dans la lettre invitant les parties à conclure.
12. Le 17 février 2021, la Chambre Contentieuse reçoit les conclusions en réponse de la défenderesse.
13. Le 5 mars 2021, la plaignante fait remarquer à la Chambre Contentieuse qu'elle n'a pas été notifiée des conclusions en réponse de la défenderesse.
14. Le 17 mars 2021, la Chambre Contentieuse fixe, en raison du problème exceptionnel de notification des conclusions à la plaignante qui est survenu, de nouveaux délais de conclusions. La nouvelle date limite pour la réception des conclusions en réplique de la plaignante est fixée au 18 avril 2021, et la nouvelle date limite pour la réception des conclusions en duplique de la défenderesse est fixée au 18 mai 2021.

15. Le 14 avril 2021, la Chambre Contentieuse reçoit les conclusions en réplique de la plaignante.
16. Le 17 mai 2021, la Chambre Contentieuse reçoit les conclusions en duplique de la part de la défenderesse.
17. Le 26 septembre 2024, les parties sont informées du fait que l'audition aura lieu le 22 octobre 2024.
18. Le 22 octobre 2024, les parties sont entendues par la Chambre Contentieuse.
19. Le 25 octobre 2024, le procès-verbal de l'audition est soumis aux parties. La Chambre Contentieuse demande également la fourniture de pièces aux parties.
20. Le 30 octobre 2024, la Chambre Contentieuse reçoit de la défenderesse quelques remarques relatives au procès-verbal qu'elle verse dans le dossier.
21. Le 6 janvier 2025, la défenderesse transmet à la Chambre Contentieuse ainsi qu'à la plaignante la documentation relative aux mesures techniques et organisationnelles qui étaient en vigueur au moment des faits, ainsi que celles actuellement en vigueur.
22. Le 27 janvier 2025, la plaignante réagit à la documentation communiquée par la défenderesse.
23. Le 11 février 2025, la défenderesse répond aux remarques formulées par la plaignante à l'égard de la documentation qu'elle a transmise en date du 6 janvier 2025.

II. Motivation

II.1. Identification du responsable de traitement

II.1.1. Le point de vue des parties

24. La plaignante identifie la défenderesse en tant que seule responsable de traitement concernant les griefs sur lesquels les parties ont été invités à conclure, à savoir, en synthèse :
 - « Quant à la base de licéité du traitement de données personnelles reproché (violation potentielle des art. 5.1.a) et 6 du RGPD) ;
 - Quant à la qualification des faits sous l'angle de l'article 33 du RGPD »².
25. La défenderesse allègue que la supérieure hiérarchique de la plaignante a agi en sa pleine autonomie lorsque celle-ci a consulté le dossier médical de la plaignante. Elle précise que cette consultation ne s'est pas faite en son nom, et qu'elle n'a nullement donné d'instruction à la supérieure hiérarchique dans la commission de cet acte. De surcroît, la défenderesse

² Lettre d'invitation à conclure du 7 janvier 2021, voy. point 10 de la présente décision.

précise que la supérieure hiérarchique a reconnu sa faute, dans le cadre de l'enquête interne qu'elle a menée³.

II.1.2. L'appréciation de la Chambre Contentieuse

26. La Chambre Contentieuse n'est pas liée par la qualité que se reconnaît la défenderesse. Elle se doit d'apprécier la réalité de cette qualification et le cas échéant de l'écarter s'il devait résulter de cette analyse que celle-ci ne peut être retenue⁴.
27. La Chambre Contentieuse rappelle qu'est défini comme un responsable de traitement « *la personne physique ou morale ou toute autre entité qui seule ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données à caractère personnel* » (art. 4.7) du RGPD). Il s'agit d'une notion autonome, propre à la réglementation en matière de protection des données dont l'appréciation doit se faire au départ des critères qu'elle énonce : la détermination des finalités du traitement de données concerné ainsi que celles des moyens de celui-ci.
28. Lorsque l'employé d'une organisation opère des traitements de données à caractère personnel dans le cadre des activités de celle-ci, le traitement est réputé avoir lieu sous l'autorité de l'organisation. Toutefois, il est des situations exceptionnelles dans lesquelles l'employé peut définir lui-même les finalités d'un traitement de données à caractère personnel, « *outrepassant ainsi de manière illicite l'autorité qui lui a été confiée* »⁵. À cet égard, il convient de préciser qu'il incombe dès lors à l'organisation en sa qualité de responsable de traitement de mettre en place les mesures techniques et organisationnelles appropriées.
29. Dans le cas de l'espèce, la Chambre Contentieuse tient compte du fait, en premier lieu, que la décision de licenciement ne s'appuyait pas sur des éléments qui auraient été collectés lors de la consultation du dossier médical de la plaignante⁶.
30. Par ailleurs, la Chambre Contentieuse note également que l'accès au dossier médical de la plaignante s'est effectué le 2 mars 2020 vers 22h50, qui ne constitue pas un horaire de travail ordinaire.
31. De surcroît, la supérieure hiérarchique a admis avoir accédé de manière fautive au dossier médical de la plaignante, et qu'elle a ainsi agi en vue de vérifier que la plaignante se trouvait

³ Voy. point 5 de la présente décision).

⁴ Voy. en ce sens Bruxelles (Cour des marchés), 8 juin 2022, 2022/AR/42, p. 6.

⁵ CEPD, Lignes directrices 07/2020 concernant les notions de responsable de traitement et de sous-traitant dans le RGPD, 7 juillet 2021, version 2, paragraphe 19, accessible via: https://www.edpb.europa.eu/system/files/2023-10/edpb_guidelines_202007_controllerprocessor_final_fr.pdf.

⁶ Voy. en ce sens la lettre du 14 avril 2020 par laquelle la défenderesse fournit les raisons qui l'ont amenée à licencier la plaignante.

dans un état adéquat afin d'apprendre son licenciement. À cet égard, la défenderesse a entamé une procédure disciplinaire à l'encontre de la supérieure hiérarchique.

32. Par voie de conséquence, la Chambre Contentieuse considère que la supérieure hiérarchique a agi en tant que seule responsable de traitement lors de la consultation du dossier médical de la plaignante, et que ce faisant elle a outrepassé l'autorité qui lui a été confiée par la défenderesse.

II.2. Quant au manquement aux articles 5.1.a) et 6 du RGPD : l'absence de base de licéité à la consultation des données de santé de la plaignante

II.2.1. Le point de vue des parties

33. La plaignante allègue que la défenderesse a consulté son dossier médical sans base de licéité valable.
34. La défenderesse déclare que la consultation du dossier médical en tant que telle est regrettable et a précisément entamé une procédure disciplinaire à l'encontre de la supérieure hiérarchique pour cela. Toutefois, la défenderesse avance ne pas être la responsable de ce traitement.

II.2.2. L'appréciation de la Chambre Contentieuse

35. Il ne convient pas d'examiner cet élément étant entendu que le traitement dont la licéité est contestée et débattue n'a pas été mis en œuvre par la défenderesse, et que le responsable de ce traitement – à savoir la supérieure hiérarchique – est tierce à la présente procédure. Pour le surplus, la Chambre Contentieuse se réfère aux points 26 à 32 de la présente décision.

II.3. Quant au manquement à l'article 33 du RGPD : l'absence de notification à l'autorité de contrôle

II.3.1. Le point de vue des parties

36. La plaignante dénonce l'absence de notification de la violation de ses données à l'APD en vertu de l'article 33 du RGPD ainsi que l'absence de documentation relative à ladite violation. À cet égard, elle relève notamment que la défenderesse n'explique pas les mesures précises qu'elle a prises à l'égard de la supérieure hiérarchique, et qu'elle n'explique pas davantage les enjeux de la procédure disciplinaire menée à l'encontre de la supérieure hiérarchique.

Enfin, elle reproche à la défenderesse de ne pas avoir documenté la violation de données conformément à l'article 33.5 du RGPD⁷.

37. La défenderesse justifie l'absence de notification à l'APD de la violation des données à caractère personnel de la plaignante par le fait qu'après une analyse conjointe entre son DPO et son service juridique, il est ressorti que ladite violation n'était pas susceptible d'entraîner un risque substantiel pour les droits et libertés de la plaignante. De surcroît, la défenderesse précise avoir averti la plaignante de cette violation. Elle relève encore que bien que des données sensibles aient été consultées de manière non autorisée, la violation se limite à la seule personne de la plaignante, que la supérieure hiérarchique n'était pas animée de mauvaises intentions et que celle-ci de toute manière a fait l'objet d'une procédure disciplinaire.
38. La défenderesse ajoute avoir documenté la violation des données à caractère personnel de la plaignante conformément à l'article 33.5 du RGPD, dans son registre des incidents.
39. En tout état de cause, la défenderesse relève que la plaignante n'allègue pas de risque précis qu'elle aurait pu encourir en conséquence de la violation de ses données à caractère personnel.

II.3.2. L'appréciation de la Chambre Contentieuse

40. L'article 4.12) du RGPD définit la «violation de données à caractère personnel» (*data breach*) comme étant « *une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, 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* ».
41. L'article 33.1 du RGPD prévoit « [qu']En cas de violation de données à caractère personnel, le responsable du traitement en notifie la violation en question à l'autorité de contrôle compétente conformément à l'article 55, dans les meilleurs délais et, si possible, 72 heures au plus tard après en avoir pris connaissance, à moins que la violation en question ne soit pas susceptible d'engendrer un risque pour les droits et libertés des personnes physiques. Lorsque la notification à l'autorité de contrôle n'a pas lieu dans les 72 heures, elle est accompagnée des motifs du retard. »⁸. Le cinquième paragraphe de cet article prévoit que « Le responsable du traitement documente toute violation de données à caractère personnel, en indiquant les faits concernant la violation des données à caractère personnel, ses effets et les mesures prises pour y remédier. La documentation ainsi constituée permet

⁷ Article 33.5 du RGPD : « *Le responsable du traitement documente toute violation de données à caractère personnel, en indiquant les faits concernant la violation des données à caractère personnel, ses effets et les mesures prises pour y remédier. La documentation ainsi constituée permet à l'autorité de contrôle de vérifier le respect du présent article.* »

⁸ C'est la Chambre Contentieuse qui souligne.

à l'autorité de contrôle de vérifier le respect du présent article.»⁹. Afin de donner de l'effectivité à ces deux dispositions, le responsable de traitement devrait également dater la documentation qui reprend cette analyse de risque.

42. La Chambre Contentieuse relève que le responsable de traitement doit en toute circonstance notifier l'APD de la violation de données à caractère personnel, à moins que celle-ci ne soit pas susceptible d'engendrer un risque pour les droits et libertés des personnes physiques. De surcroît, il convient de comprendre que cette notification est de principe, et que le fait de ne pas notifier l'APD de la violation en question est l'exception dont le responsable doit démontrer que les conditions d'application sont effectivement réunies dans une situation donnée. En tout état de cause, dans un souci de prudence et une perspective protectrice des droits et libertés des personnes concernées, un responsable de traitement devrait toujours, en cas de doute, notifier l'APD d'une violation de données dans un délai de 72 heures lorsqu'il est informé de celle-ci, même dans les cas où il considère pour plusieurs raisons que la violation n'est pas susceptible d'engendrer de risque pour les droits et libertés de la personne concernée, mais qu'eu égard aux circonstances de l'espèce, il ne peut pas en être tout à fait certain¹⁰.
43. La Chambre Contentieuse constate que les données à caractère personnel de la plaignante ont fait l'objet d'un accès non-autorisé (violation de confidentialité) par la supérieure hiérarchique, et que de surcroît des données de santé figuraient parmi celles-ci, lesquelles sont protégées notamment par l'article 9 du RGPD et le secret professionnel, et appellent à une vigilance toute particulière. Elle ajoute que la défenderesse ne lui a pas transmis la documentation constituée conformément à l'article 33.5 du RGPD.
44. Il découle du considérant 75 du RGPD qu'un risque entendu au sens de l'article 33 du même Règlement peut ressortir « *en particulier : [...] lorsque le traitement peut donner lieu à une discrimination, à un vol ou une usurpation d'identité, à une perte financière, à une atteinte à la réputation, à une perte de confidentialité de données protégées par le secret professionnel, [...] lorsque le traitement concerne des données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, la religion ou les convictions philosophiques, l'appartenance syndicale, ainsi que des données génétiques, des données concernant la santé ou des données concernant la vie sexuelle ou des données relatives à des condamnations pénales et à des infractions, ou encore à des mesures de sûreté connexes; »¹¹.*

⁹ C'est la Chambre Contentieuse qui souligne.

¹⁰ CEPD, Lignes directrices 9/2022 sur la notification de violations données à caractère personnel en vertu du RGPD, Version 2.0, adoptées le 28 mars 2023, paragraphe 119, disponible via : https://www.edpb.europa.eu/system/files/2024-10/edpb_guidelines_202209_personal_data_breach_notification_v2.0_fr_0.pdf.

¹¹ C'est la Chambre qui souligne.

45. La Chambre Contentieuse considère que le fait que la violation de données ne concernait que la seule personne de la plaignante, que la défenderesse a entamé une procédure disciplinaire à l'égard de la supérieure hiérarchique qui a reconnu avoir agi fautivement et que celle-ci n'avait supposément pas d'intention malveillante lorsqu'elle a accédé de manière inappropriée au dossier médical de la plaignante ne suffisent pas en l'espèce à décharger la défenderesse de son obligation de notifier l'autorité de contrôle de la violation des données telle qu'elle ressort du cas d'espèce.
46. En effet, bien que la supérieure hiérarchique ait avancé avoir été guidée par des motivations qui peuvent apparaître comme étant louables dans le cadre de son accès inapproprié au dossier médical de la plaignante, la défenderesse ne pouvait pour autant pas être certaine que la supérieure hiérarchique n'a pas opéré cet accès pour des raisons cachées ou n'a pas prévu des traitements ultérieurs. En toute hypothèse, certains risques se sont déjà matérialisés étant entendu que la plaignante a subi une perte de contrôle et de confidentialité sur des données la concernant, lesquelles sont protégées par le secret professionnel. Dès lors, les considérations se trouvant ci-avant ont davantage égard à la question de la gravité des risques, et non de la possibilité des risques en elle-même. À ce titre, l'on ne pourrait retenir la circonstance que la plaignante fût la seule personne concernée par la violation de données étant entendu que s'il est certes admis que les conséquences d'une violation de données peuvent être plus nombreuses si le nombre de personnes concernées est élevé, l'on ne pourrait pour autant parvenir à la conclusion que la violation de données limitée à une seule personne concernée ne pourrait pas entraîner de risque sur les droits et libertés de celle-ci. Cela est de toute évidence le cas lorsque des données relatives à la santé de la personne concernée sont impliquées dans la violation de données, et que le responsable de traitement ne peut avoir de certitude sur les motivations qui ont poussé la personne qui a commis l'accès inapproprié aux données concernées à le faire.
47. Cependant, la Chambre Contentieuse prend en compte que les faits sont survenus vers le début de l'année 2020 ; qu'à ce moment, le RGPD n'était entré en application que depuis moins de deux ans, que le CEPD n'avait encore publié ni ses lignes directrices 01/2021 *relatives aux exemples concernant la notification de violations de données à caractère personnel* ni son actualisation des lignes directrices WP250 adoptées le 3 octobre 2017 *sur la notification de violations de données à caractère personnel en vertu du règlement (UE) 2016/679* en les lignes directrices 9/2022 *sur la notification de violations de données à caractère personnel en vertu du RGPD*, et que d'une manière plus générale le niveau de la connaissance et de la pratique concernant la gestion des violations de données à caractère personnel ne se trouvait pas au même niveau qu'aujourd'hui. Par conséquent, la Chambre Contentieuse considère que compte tenu du contexte dans lequel se trouvait la

défenderesse, il ne pourrait pas lui être reproché de ne pas avoir notifié l'APD de la violation des données de la plaignante conformément à l'article 33 du RGPD au moment des faits.

48. La Chambre Contentieuse précise toutefois que le niveau actuel de la connaissance et de la pratique concernant la gestion des violations de données à caractère personnel se trouve à un stade tel que si des faits similaires devaient survenir à nouveau, alors le responsable de traitement ne pourrait faire valoir l'exception prévue par l'article 33 du RGPD, et qu'il ne pourrait donc pas se décharger de son obligation de notifier l'APD en cas de violation de données au motif que celle-ci ne comporterait pas de risque pour les droits et libertés de la personne concernée.

II.4. Quant aux mesures techniques et organisationnelles de la défenderesse

49. Au terme de l'audition qui s'est tenue le 22 octobre 2024, la défenderesse a été invitée à communiquer les mesures techniques et organisationnelles qui étaient en vigueur au moment de la survenance des faits concernant les aspects relatifs à l'accès aux dossiers médicaux par son personnel, ainsi que celles en vigueur à ce jour. Les parties ont ensuite pu valablement échanger à cet égard. La Chambre Contentieuse précise que les parties n'ont pas été invitées à conclure à propos des aspects relatifs aux mesures techniques et organisationnelles de la défenderesse dans le cadre de la lettre qu'elle leur a adressée le 7 janvier 2021, et que dès lors la Chambre Contentieuse prendra pas de décision concernant cet aspect.

II.4.1. Le point de vue des parties

50. En premier lieu, la défenderesse relève que les mesures techniques et organisationnelles n'ont pas évolué depuis la survenance des faits à l'origine du cas d'espèce, ce que la plaignante dénonce.
51. Concernant celles-ci, la défenderesse expose qu'un lien thérapeutique est présumé exister pour l'ensemble de ses professionnels de soins de santé. Elle relève que son personnel est pluridisciplinaire, qu'il y a du personnel médical mais aussi paramédical, et qu'au cours de la prise en charge des patients ceux-ci sont amenés à devoir être traités par de multiples praticiens. Elle ajoute que le fait pour ses employés de ne pas pouvoir connaître des informations adéquates relatives aux patients pourrait porter atteinte à la continuité des soins. C'est pour cette raison que la défenderesse justifie que l'entièreté du personnel médical et paramédical dispose par défaut d'un accès au logiciel Oribase, et donc d'un accès aux dossiers médicaux de l'intégralité de ses patients. En toute hypothèse, les accès aux dossiers médicaux sont tracés informatiquement.

52. La défenderesse ajoute que ces mesures techniques et organisationnelles sont destinées à évoluer. En effet, le logiciel qu'elle utilise depuis au moins la survenance des faits, à savoir « Oribase », va être remplacé par le « Portail Patient » lors de sa fusion avec deux autres hôpitaux.
53. Quant à ce nouveau logiciel, la défenderesse relève plusieurs mesures qui y seront implémentées, lesquelles peuvent être résumées comme suit :
- Pour chaque demande d'accès apparaîtra une fenêtre d'avertissement demandant à la personne concernée si elle entretient bien un lien thérapeutique avec la personne dont elle souhaite accéder au dossier médical ;
 - Lorsque la personne qui cherche à accéder à un dossier médical a un profil administratif, alors cette personne doit fournir un justificatif ;
 - Il faut toujours fournir un justificatif lorsqu'un employé de la défenderesse cherche à accéder au dossier d'un membre du personnel ;
 - À l'ouverture du dossier d'un patient, une partie de l'écran donnera des informations sur les cinq derniers accès au même dossier ;
 - Il y aura également une redéfinition des profils et des accès aux dossiers médicaux.
54. La défenderesse a également partagé (i) la présentation qu'elle assure chaque mois pour les nouveaux employés relative au respect de confidentialité des dossiers médicaux et du fait que les employés ne peuvent consulter des dossiers médicaux qu'en cas de lien thérapeutique, ainsi (ii) qu'une formation obligatoire sous forme d'e-learning qui existe depuis le 1^{er} janvier 2024 pour tous les nouveaux arrivants. Elle fait également des sensibilisations ponctuelles à tout le personnel par le biais de *newsletters*.
55. En outre, elle a également partagé deux lettres¹² par lesquelles elle informait les destinataires de leur licenciement pour faute grave, celle-ci consistant en la consultation inappropriée de dossiers médicaux. La lettre la plus récente est datée au 24 juillet 2024.

II.4.2. L'appréciation de la Chambre Contentieuse

56. La Chambre Contentieuse relève que la défenderesse traite d'un très large nombre de données de santé étant entendu qu'elle est une institution hospitalière, et que celles-ci, comme cela a été dit au point 43, appellent à une vigilance toute particulière.

¹² Pièces 6 et 7 du dossier de pièces que la défenderesse a fourni à la Chambre Contentieuse et à la plaignante le 6 janvier 2025. La Chambre Contentieuse relève que les deux pièces sont exactement identiques, toutefois la pièce 6 est intitulée « pièce 6 lettre de licenciement pour faute grave en date du 24 janvier 2022 » tandis que la pièce 7 est intitulée « Pièce 7 lettre de licenciement pour faute grave en date du 24 juillet 2024 ». En outre, la défenderesse fait bien référence à ces deux pièces distinctement dans ses lettres. Dès lors, la Chambre Contentieuse considère que le fait que les deux pièces soient identiques n'est que le résultat d'une erreur matérielle.

57. L'article 5.1.f) du RGPD prévoit que les données à caractère personnel sont « *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)* », et qu'en vertu de l'article 5.2 du RGPD les responsables doivent être en mesure de démontrer respecter le premier paragraphe de l'article 5 du RGPD (principe d'*accountability*).
58. L'article 24 du RGPD expose en ses deux premiers paragraphes que : « 1. *Compte tenu de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques, le responsable du traitement met en œuvre des mesures techniques et organisationnelles appropriées pour s'assurer et être en mesure de démontrer que le traitement est effectué conformément au présent règlement. Ces mesures sont réexaminées et actualisées si nécessaire.*
2. *Lorsque cela est proportionné au regard des activités de traitement, les mesures visées au paragraphe 1 comprennent la mise en œuvre de politiques appropriées en matière de protection des données par le responsable du traitement.* »¹³.
59. L'article 32.1 du RGPD prévoit que « *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 (...)* »¹⁴. Le cinquième paragraphe de l'article 32 dispose que « *Le responsable du traitement et le sous-traitant prennent des mesures afin de 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.* »¹⁵.
60. Dans le cas de l'espèce, la Chambre Contentieuse constate que le dossier médical de la plaignante a été consulté par sa supérieure hiérarchique sans que le traitement ne vise une finalité relative à un éventuel suivi du diagnostic ou un éventuel suivi thérapeutique de la plaignante. Il ne ressort d'aucune pièce du dossier que la supérieure hiérarchique ait jamais fait partie d'un des groupes du personnel de la défenderesse qui était responsable de la prise en charge médicale de la plaignante, ce qui aurait alors pu démontrer qu'il était

¹³ C'est la Chambre Contentieuse qui souligne.

¹⁴ C'est la Chambre Contentieuse qui souligne.

¹⁵ C'est la Chambre Contentieuse qui souligne.

médicalement nécessaire pour la supérieure hiérarchique de consulter le dossier médical de la plaignante. De surcroît, la circonstance que la plaignante se trouvait dans un lien de subordination avec sa supérieure hiérarchique constituait en soi une raison impérieuse pour cette dernière de ne pas consulter le dossier médical de la plaignante, sauf circonstance exceptionnelle.

61. La Chambre Contentieuse ajoute dès lors qu'il est possible que les mesures techniques et organisationnelles qui étaient en vigueur au moment des faits n'étaient pas suffisantes, et ce surtout parce que la consultation inappropriée du dossier médicale de la plaignante n'a été détectée qu'après que cette dernière en ait soulevé la question auprès de la défenderesse, toutefois, la Chambre Contentieuse précise que ces mesures techniques et organisationnelles ne peuvent pas non plus conduire à la mise en péril de la continuité des soins des patients, ce qui pourrait placer la santé de ces derniers en danger. Aussi, comme la défenderesse l'allègue (voy. point 51 de la présente décision), il n'est pas toujours possible de déterminer à l'avance quels membres du personnel médical ou paramédical d'un hôpital – lequel personnel est pluridisciplinaire – seront amenés à entrer en contact avec un patient, ce qui justifie que l'ensemble du personnel médical et paramédical dispose d'un accès aux dossiers médicaux des patients de l'hôpital.
62. De surcroît, par une lettre du 24 juillet 2024¹⁶ la défenderesse énonçait les différentes fautes retenues dans le cadre du licenciement pour faute grave de l'un de ses employés. En synthèse, il apparaît que l'ex-employé qui a fait l'objet de ce licenciement l'a été parce qu'il a consulté de manière inappropriée à plusieurs dossiers médicaux de ses ex-collègues. Dès lors, des consultations inappropriées se sont répétées.
63. Toutefois, la Chambre Contentieuse relève que dans le cadre de ce licenciement, cette fois-ci la défenderesse a pu rapidement prendre connaissance de ces accès inappropriés aux dossiers médicaux de membres du personnel, et qu'elle a rapidement pris des mesures adéquates, à savoir en particulier la décision de licenciement. Elle a ainsi agi de manière appropriée et proactive.
64. En tout état de cause, la Chambre Contentieuse tient compte du fait que, comme l'a indiqué la défenderesse, ces mesures techniques et organisationnelles sont destinées à évoluer.

III. Mesures correctrices et sanctions

65. Au terme de l'article 100, § 1^{er} de la LCA, la Chambre Contentieuse a le pouvoir de :
 - 1° classer la plainte sans suite ;
 - 2° ordonner le non-lieu ;

¹⁶ Pièce 7 du dossier que la défenderesse a transmis à la Chambre Contentieuse et à la plaignante le 6 janvier 2025.

- 3° prononcer une suspension du prononcé ;
- 4° proposer une transaction ;
- 5° formuler des avertissements ou des réprimandes ;
- 6° ordonner de se conformer aux demandes de la personne concernée d'exercer ses droits;
- 7° ordonner que l'intéressé soit informé du problème de sécurité ;
- 8° ordonner le gel, la limitation ou l'interdiction temporaire ou définitive du traitement ;
- 9° ordonner une mise en conformité du traitement ;
- 10° ordonner la rectification, la restriction ou l'effacement des données et la notification de celles-ci aux récipiendaires des données ;
- 11° ordonner le retrait de l'agrément des organismes de certification ;
- 12° donner des astreintes ;
- 13° donner des amendes administratives ;
- 14° ordonner la suspension des flux transfrontières de données vers un autre Etat ou un organisme international.

66. Au regard des deux potentielles violations au RGPD sur lesquelles les parties ont été invitées à conclure, la Chambre Contentieuse décide **d'ordonner le non-lieu** étant entendu que, d'une part, concernant l'aspect relatif à la licéité du traitement consistant en la consultation du dossier médical de la plaignante, la défenderesse ne saurait être considérée comme le responsable de ce traitement, et, d'autre part, concernant l'aspect relatif à la notification de la violation de données (art. 33 du RGPD) il ne pourrait être reproché de faute à la défenderesse eu égard au contexte dans lequel se trouvait la défenderesse, bien que la Chambre Contentieuse précise que si des faits similaires devaient de nouveau survenir, alors il conviendrait d'en notifier l'APD conformément à l'article 33 du RGPD.

IV. Publication de la décision

67. Vu l'importance de la transparence concernant le processus décisionnel de la Chambre Contentieuse, la présente décision est publiée sur le site Internet de l'Autorité de protection des données. Toutefois, il n'est pas nécessaire à cette fin que les données d'identification des parties soient directement communiquées.

PAR CES MOTIFS,

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

- En vertu de l'article 100, § 1^{er}, 2° de la LCA, **d'ordonner le non-lieu** de cette affaire.

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 1034^{ter} du Code judiciaire¹⁷. La requête interlocutoire doit être déposée au greffe de la Cour des Marchés conformément à l'article 1034^{quinquies} du C. jud.¹⁸, ou via le système d'information e-Deposit du Ministère de la Justice (article 32^{ter} du C. jud.).

(Sé). Hielke HIJMANS

Président de la Chambre Contentieuse

¹⁷ 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.

¹⁸ 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.