Autorité de protection des données
Gegevensbeschermingsautoriteit

Chambre Contentieuse

Décision 103/2023 du 26 juillet 2023

Numéro de dossier : DOS-2022-03592

Objet : Plainte relative à l'accessibilité à des données concernant la santé d'un patient à l'ensemble du personnel d'un hôpital

La Chambre Contentieuse de l'Autorité de protection des données, constituée de monsieur Hielke Hijmans, président;

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

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

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

Vu les pièces du dossier ;

A pris la décision suivante concernant :

La plaignante : Madame X, ci-après « la plaignante » ;

La défenderesse : Le Centre Hospitalier Y, ci-après : « la défenderesse».

I. Faits et procédure

1. L'objet de la plainte concerne l'accès aux données de la plaignante par des membres du personnel de la défenderesse autres que ceux et celles ayant pris en charge la plaignante lors de sa visite initiale auprès d'un centre spécialisé de la défenderesse.

2. Le 3 septembre 2022 le plaignant a introduit une plainte auprès de l'Autorité de protection des données (APD) contre la défenderesse.

3. Le 5 septembre 2022, la plainte est déclarée recevable par le Service de Première Ligne (SPL) de l'APD sur la base des articles 58 et 60 de la LCA[1] et la plainte est transmise à la Chambre Contentieuse en vertu de l'article 62, § 1er de la LCA[2].

4. La plaignante expose qu'à la suite d'une agression sexuelle, elle s'est en septembre /octobre 2021 rendue au Centre Z , un centre spécialisé de la défenderesse[3].

5. La plaignante précise également qu'environ 8 mois plus tard, le 19 avril 2022, elle s'est rendue à une consultation psychologique auprès de la défenderesse. Cette consultation a eu lieu dans le contexte de sa grossesse et de la préparation à l'accouchement à venir, sans lien expose-t-elle avec la violence sexuelle vécue. La plaignante indique que lors de cette consultation, la psychologue lui a posé un certain nombre de questions sur l'agression sexuelle dont elle avait été victime. La plaignante indique en avoir déduit que, manifestement, la psychologue avait eu accès aux informations détenues par le centre Z à la suite de son passage en septembre /octobre 2021 (point 4). La plaignante rapporte s'être inquiétée de cette situation et du fait qu'un grand nombre de personnes (membres du personnel de la défenderesse, médecins, …) semblait ainsi pouvoir accéder à des données très délicates et sensibles la concernant.

6. La plaignante expose encore que le jour même, elle a oralement contacté le centre Z qui lui a indiqué que l'ensemble du personnel médical de la défenderesse pouvait accéder au résumé de sa consultation au centre Z (en ce compris dès lors selon la plaignante aux détails de l'agression sexuelle dont elle avait été victime). La plaignante dit avoir sollicité que seul le centre Z ait accès aux dites informations. Elle rapporte qu'il lui a été répondu que ce n'était alors pas possible mais qu'une procédure était en cours pour rendre ce type de données moins accessibles et qu'à terme, seules les données relatives à la dispense de l'un ou l'autre médicament par exemple seraient accessibles et non plus l'intégralité du dossier. La

[1] En vertu de l'article 61 LCA, la Chambre Contentieuse informe les parties par la présente décision, du fait que la plainte a été déclarée recevable.

[2] En vertu de l'article 95, § 2 LCA, par la présente décision, la Chambre Contentieuse informe les parties du fait qu'à la suite de cette plainte, le dossier lui a été transmis.

[3] [……] : référence du site Internet du centre spécialisé Z de la défenderesse.

plaignante ajoute qu'il ne lui a pas été précisé si ce nouveau régime s'appliquerait aux dossiers déjà ouverts (tels le sien) ou non.

7. La plaignante produit à l'appui de sa plainte le courriel qu'elle a ensuite, deux mois plus tard, soit le 20 juin 2022, écrit au délégué à la protection des données (DPO) de la défenderesse aux termes duquel elle relate ce qui précède (points 5 et 6) et pose la question du délai dans lequel le nouveau régime sera d'application et s'il visera des dossiers tels que le sien. De manière générale, la plaignante exprime qu'elle a le sentiment que cette large accessibilité *« (…) va à l'encontre de mes droits à la vie privée, précisément lorsque cela touche à des données sensibles tels que le descriptif d'une agression sexuelle ».*

8. Par correction, la plaignante a le même jour (20 juin 2022), informé le centre Z de la démarche qu'elle avait faite auprès du DPO de la défenderesse, lui adressant une copie du courriel envoyé. Elle s'est également assurée auprès du centre Z que les propos qu'elle relatait au DPO à la suite de la conversation qu'elle avait eue avec le centre reflétait bien la réalité. Ce courriel est également produit au dossier.

9. Le 21 juin 2022, un membre du centre Z confirmait à la plaignante que le compte-rendu de la situation qu'elle avait exposé était effectivement fidèle à la réalité. Il a par ailleurs été précisé à la plaignante d'une part que la modification des dossiers du Centre Z devrait être réalisée dans le courant de l'année 2022 au plus tard dans un délai de 6 mois, la démarche demandant du temps et de l'investissement et d'autre part qu'elle serait le cas échéant informée de nouvelles informations utiles la concernant. Ce mail est produit au dossier.

10. De son côté, le DPO de la défenderesse a indiqué par retour de mail du 20 juin à la plaignante qu'une réunion était fixée dans les semaines à venir avec le Centre Z afin d'analyser sa situation et qu'à la suite de cette réunion, un courrier lui serait transmis concernant l'accès à ses données liées à l'agression sexuelle dont elle a été victime. Très précisément, le DPO écrit ce qui suit à la plaignante : *« Une réunion est fixée ce … avec … [le centre Z] afin d'analyser votre situation. Suite à cette réunion, un courrier vous sera transmis concernant l'accès de vos données liés à l'agression (blocage de l'accès aux détails des faits)* [4]».

11. Au moment de déposer plainte à l'APD le 3 septembre 2022, la plaignante indique ne pas avoir reçu de suivi de la part (du DPO) de la défenderesse.

II. Motivation

12. La Chambre Contentieuse conclut que les données relatives à l'agression sexuelle dont la plaignante rapporte avoir été victime sont des données à caractère personnel la concernant au sens de l'article 4.1. du RGPD. Certaines d'entre-elles sont, selon toute vraisemblance,

[4] C'et la Chambre Contentieuse qui souligne.

relatives à sa santé au sens de l'article 9.1. du RGPD et du considérant 43 de celui-ci. D'autres données plus factuelles, liées à la description des faits d'agression par exemple, ne sont potentiellement pas sensibles au sens de l'article 9.1. du RGPD. La Chambre Contentieuse n'en est pas moins d'avis que ces données sont, dans le contexte de violence sexuelle dont la plaignante a été victime, des « données à caractère hautement personnel » au sens que donne le Comité européen de la protection des données (CEPD) à cette notion[5]. La plus grande vigilance quant au respect du RGPD doit être de mise à leur égard.

13. La Chambre Contentieuse relève qu'il ressort également de la plainte et des pièces produites par la plaignante qu'il y a bien « traitement » de données au sens de l'article 4.2. du RGPD, les données personnelles de la plaignante étant conservées et accessibles électroniquement.

14. Sur la base de la politique de confidentialité de la défenderesse[6], la Chambre Contentieuse estime, *prima facie*, que la défenderesse est le responsable de traitement présumé des traitements de données de la plaignante, en ce compris ceux réalisés par le Centre Z .

15. Tout responsable de traitement est tenu de respecter l'article 24 du RGPD qui implique que 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 de traitement mette en œuvre des mesures techniques et organisationnelles appropriées pour s'assurer et être en mesure de démontrer que le traitement est effectué conformément au RGPD. Tout responsable de traitement doit par ailleurs être en mesure de le démontrer (article 5.2. du RGPD).

16. Le responsable de traitement est également soumis à l'obligation de sécurité prévue à l'article 32 du RGPD.

17. L'article 32 du RGPD spécifie quant à lui 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 de traitement et le sous-traitant mettent en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un haut niveau de sécurité adapté au risque, y compris entre autres selon les besoins : (...) b) des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement*. (...)[7] ».

---

[5] Groupe de l'Article 29, Lignes directrices concernant l'analyse d'impact relative à la protection des données (AIPD) et la manière de déterminer si le traitement est «susceptible d'engendrer un risque élevé» aux fins du règlement (UE) 2016/679, WP 248. Los de sa séance inaugurale le Comité européen de la protection des données a endossé ces lignes directrices : https://ec.europa.eu/newsroom/article29/items/611236

[6] [.....] : référence de la politique de confidentialité de la défenderesse disponible sur son site Internet.

[7] C'est la Chambre Contentieuse qui souligne.

18. La confidentialité est la propriété d'une information de ne pouvoir être accédée que par des personnes, entités ou processus autorisés et de ne pouvoir être divulguée qu'à des personnes, entités ou processus autorisés. Cette possibilité d'accorder un accès sélectif aux informations doit être assurée tout au long de la vie de ces informations notamment au cours de leurs collectes, de leur conservation, de leurs traitements et de leurs communications. En pratique, les seules personnes autorisées à accéder aux données à caractère personnel sont les personnes dont la fonction ou les activités professionnelles justifient cet accès.[8]

19. Il découle ainsi de l'article 32 du RGPD lu conjointement avec l'article 24 du RGPD que la défenderesse était et demeure tenue de mettre en oeuvre toutes les mesures techniques et organisationnelles de nature à garantir que les prestataires de soins et autres professionnels qui recourent à son système d'échange d'information n'accèdent qu'aux seules données du dossier de patient nécessaires à leurs prestations respectives et ce, dans le respect de l'ensemble du cadre juridique applicable dont, mais non exclusivement, le RGPD.

20. Dans sa recommandation CM/Rec(2019)2[9], le Comité des ministres du Conseil de l'Europe[10] recommande dans le même sens ce qui suit: *« l'échange et le partage de données relatives à la santé entre professionnels de santé devraient être limités aux informations strictement nécessaires à la coordination ou la continuité des soins, à la prévention ou au suivi médico-social et social de la personne. Chaque professionnel de santé ne peut, dans ce cas, transmettre ou recevoir que les données qui relèvent du périmètre de ses missions, en fonction de ses habilitations. Des mesures appropriées devraient être prises afin de garantir la sécurité des données. L'utilisation d'un dossier médical électronique et d'une messagerie électronique de nature à* permettre le partage et l'échange de données relatives à la santé devrait respecter ces principes ».

21. De manière générale, l'accès à des données hébergées sur un serveur tel celui d'un hôpital doit prendre en considération plusieurs critère et conditions déterminants tels que l'identité et la qualité du demandeur d'accès, le type de données concernées, le degré de confidentialité de celles-ci, la finalité de la demande et la durée de l'accès. Le serveur devra

---

[8] Voy. à cet égard la note relative à la sécurité de l'information de l'APD https://www.autoriteprotectiondonnees.be/publications/note-relative-a-la-securite-des-donnees-a-caractere-personnel.pdf

[9] https://search.coe.int/cm/pages/result_details.aspx?ObjectId=090000168093b26b. La Chambre Contentieuse estime que le contenu de cette note (rédigée à un moment où le RGPD n'était pas encore en application) reste pertinent au regard des principes de sécurité qu'elle énonce.

[10] Le cadre de référence en matière de protection des données du Conseil de l'Europe n'est certes pas le RGPD mais bien la Convention 108 (Convention pour le protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STE n° 108) : https://rm.coe.int/1680078b39) et bientôt, une fois en vigueur, la Convention 108+ (Protocole d'amendement à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel – STE 223 : https://www.coe.int/fr/web/conventions/full-list?module=treaty-detail&treatynum=223). Ces textes n'en contiennent pas moins des principes comparables en matière de protection des données et de sécurité à ceux du RGPD et sont autant de sources d'inspiration quant aux mesures à mettre en place par un responsable de traitement dans une situation telle que celle de la plainte.

intégrer ces différents facteurs de manière à ce que les accès soient filtrés et réservés à ceux qui y sont autorisés dans le respect du RGPD et d'autres normes auxquelles les accédants sont respectivement tenus[11].

22. La Chambre Contentieuse relève à cet égard que la plaignante a intitulé l'objet des courriels qu'elle produit en complément du formulaire de plainte déposé comme suit : « *secret professionnel partagé dans le cadre de violences sexuelles* « .

23. La Chambre Contentieuse n'est certes pas compétente pour sanctionner une éventuelle violation de l'article 458 du code pénal (secret professionnel) en tant que telle ni pour apprécier le respect des conditions du secret professionnel partagé. Elle l'est en revanche pour vérifier que le système d'échange d'information mis en place par la défenderesse garantit des accès aux données personnelles des patients dans le respect du principe de sécurité tel que rappelé ci-dessus, dont la confidentialité à laquelle le respect du secret professionnel participe sans se confondre avec lui.

24. La Chambre Contentieuse rappelle ici qu'à plusieurs reprises la Cour européenne des droits de l'homme a insisté sur l'importance que revêt le respect du secret professionnel non seulement pour la vie privée des patients mais également plus généralement pour le droit à la santé[12].

---

[11] Voy. également à titre d'exemple, le Règlement approuvé par le Comité de gestion de la plateforme eHealth le 10 septembre 2019 et le Comité de sécurité de l'information le 7 avril 2020 ainsi que la délibération du Comité de sécurité de l'information (Délibération 19/166 du 1er octobre 2019, modifiée le 6 juillet 2021) – cercles de confiance (circle of trust) : https://www.ehealth.fgov.be/ehealthplatform/file/view/AW0kmXp0gwvToiwBkkgH?filename=R%C3%A8glement%20COT%20-%2005032021%20-%20v2.pdf

[12] De l'arrêt *Niemietz c. Allemagne du 16 décembre 1992*, on a ainsi pu déduire que la Cour européenne des droits de l'homme (Cour eur. D.H.) avait, fut-ce implicitement, mis en relief une double fonction du secret professionnel (en l'espèce de l'avocat) : (1) la confidentialité des rapports entre e professionnel soumis au secret professionnel (l'avocat) et son client est protectrice des droits subjectifs déduits de l'article 8 (vie privée) mais (2) également garante du bon fonctionnement de la justice (fondement social).[12] Dans l'arrêt *Z. c. Finlande*[12], la Cour eur. D.H. aborde, pour la première fois, à tout le moins directement[12], la question du secret médical. Dans cet arrêt, le même double fondement préside à l'appréhension du secret médical par la Cour. Elle y indique qu'elle tiendra compte du rôle fondamental que joue la protection des données à caractère personnel – les informations médicales n'en étant pas les moindres – pour l'exercice du droit au respect de la vie privée et familiale garanti par l'article 8 de la Convention européenne des droits de l'homme (CEDH). Le respect du caractère confidentiel des informations sur la santé constitue un principe essentiel du système juridique de toutes les Parties contractantes à la CEDH. Il est capital non seulement pour protéger la vie privée des malades mais également pour préserver leur confiance dans le corps médical et les services de santé en général . La Cour fait preuve d'innovation terminologique en exigeant, pour toute justification éventuelle à l'atteinte au secret professionnel, la défense *« d'un aspect primordial de l'intérêt public »* (§96) et en déclarant qu'elle exercera en la matière *« un contrôle des plus rigoureux »* (§96). En d'autres termes, le secret professionnel est destiné à protéger la confidentialité de l'échange entre le patient et le professionnel des soins de santé soumis au secret à qui il s'adresse - en n'en divulguant pas le contenu à des tiers non autorisés – et ce, non seulement dans l'intérêt du confident mais également dans celui de la société dans son ensemble.

25. Ainsi que la Commission de la protection de la vie privée (CPVP) l'énonçait dans sa note relative à la sécurité (voir note 6), *« La sécurité est certainement d'abord une affaire de direction »* en ce que l'élaboration et la mise en place d'un processus de sécurisation efficace requiert la pleine conscience de la direction et des différents responsables, dont notamment le responsable de traitement, du rôle primordial que joue la sécurité au sein de l'entité concernée ainsi que leur totale adhésion aux objectifs de sécurité recherchés et leur collaboration active.

26. Toujours comme souligné dans ladite note, *« La sécurité est ensuite l'affaire de tous »* : tous les membres de l'organisation, quels qu'ils soient, font tous partie, un moment ou l'autre, de la chaîne de sécurité et risquent, de ce fait, d'en être un jour le maillon faible. Chacun doit être conscientisé et responsabilisé de son propre rôle dans cette chaîne, et doit être préparé, sensibilisé et formé en conséquence. Cette conscientisation doit être mise en place par le responsable de traitement avec le concours de son délégué à la protection des données (DPO).

27. S'agissant du cas d'espèce, la Chambre Contentieuse relève qu'il semble ressortir des échanges de courriels produits par la plaignante que l'ensemble du personnel de la défenderesse ait potentiellement accès aux données personnelles la concernant, à tout le moins celles dont elle fait état relativement à l'agression sexuelle dont elle a été victime. Il n'appartient pas à la Chambre Contentieuse de conclure que l'accès qu'a opéré la psychologue aux données de la plaignante (point 4) était ou non nécessaire à ses prestations professionnelles. En revanche, si la défenderesse ne devait pas disposer d'une politique d'accès aux données des dossiers médicaux qui soit conforme au RGPD et plus particulièrement au principe de sécurité lu en combinaison avec le principe d'accountability, la défenderesse se rendrait coupable de violation de ces dispositions.

28. Compte tenu de ce qu'il se dégage des pièces produites par la plaignante que la défenderesse semble être engagée dans un processus d'adaptation de sa politique d'accès, la Chambre Contentieuse estime que lui adresser un avertissement est la mesure correctrice la plus appropriée au cas d'espèce. La mise en œuvre de cette politique d'accès conforme au RGPD devrait selon la Chambre Contentieuse s'appliquer également aux dossiers déjà ouverts auprès de la défenderesse et ce, le plus rapidement possible en tenant compte de la haute sensibilité des données de la plaignante.

29. En conclusion, la Chambre Contentieuse estime que sur la base des faits susmentionnés, il y a lieu de conclure que la défenderesse peut avoir commis une violation des dispositions du RGPD, ce qui justifie qu'en l'occurrence, la Chambre Contentieuse procède à la prise d'une décision conformément à l'article 95, § 1er, 4° de la LCA, soit plus précisément à l'adoption d'une décision d'avertissement.

30. La présente décision est une décision *prima facie* prise par la Chambre Contentieuse conformément à l'article 95 de la LCA sur la base de la plainte introduite par la plaignante, dans le cadre de la « *procédure préalable à la décision de fond* »[13] . Il ne s'agit pas d'une décision sur le fond de la Chambre Contentieuse au sens de l'article 100 de la LCA.

31. En application de l'article 95 § 2, 3° de la LCA ainsi que l'article 47 du règlement d'ordre intérieur de l'APD, une copie du dossier peut être demandée par les parties. Si l'une des parties souhaite faire usage de la possibilité de consulter ce dossier, elle est tenue de s'adresser au secrétariat de la Chambre contentieuse, de préférence via l'adresse litigationchamber@apd-gba.be.

32. La présente décision *prima facie* a pour but d'informer la défenderesse, présumée responsable du traitement, du fait qu'elle peut avoir commis une violation des dispositions du RGPD, afin de lui permettre d'encore se conformer aux dispositions précitées.

33. Si la défenderesse ne devait toutefois pas être d'accord avec le contenu de la présente décision *prima facie* et devait estimer qu'elle peut faire valoir des arguments factuels et/ou juridiques qui pourraient conduire à une autre décision, elle peut adresser à la Chambre Contentieuse une demande de traitement sur le fond de l'affaire via l'adresse litigationchamber@apd-gba.be, et ce dans le délai de 30 jours après la notification de la présente décision. Le cas échéant, l'exécution de la présente décision sera suspendue pendant la période susmentionnée.

34. En cas de poursuite du traitement de l'affaire sur le fond, en vertu des articles 98, 2° et 3° *juncto* l'article 99 de la LCA, la Chambre Contentieuse invitera les parties à introduire leurs conclusions et à joindre au dossier toutes les pièces qu'elles jugeront utiles. Le cas échéant, la présente décision sera définitivement suspendue.

35. Dans une optique de transparence, la Chambre Contentieuse souligne enfin qu'un traitement de l'affaire sur le fond peut conduire à l'imposition des mesures mentionnées à l'article 100 de la LCA[14].

---

[13] Section 3, Sous-section 2 de la LCA (articles 94 à 97 inclus).

[14] Art. 100. § 1er. La chambre contentieuse a le pouvoir de
1° classer la plainte sans suite ;
2° ordonner le non-lieu ;
3° prononcer la suspension du prononcé ;
4° proposer une transaction ;
5° formuler des avertissements et 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'agréation 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 État ou un organisme international ;

III. Publication de la décision

36. 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'APD. Toutefois, il n'est pas nécessaire à cette fin que les données d'identification des parties soient directement mentionnées.

PAR CES MOTIFS,

la Chambre Contentieuse de l'Autorité de protection des données décide, sous réserve de l'introduction d'une demande par la défenderesse d'un traitement sur le fond conformément aux articles 98 e.s. de la LCA :

- en vertu de l'article **58.2.c)** du RGPD et de l'article **95, § 1er, 4°** de la LCA, d'adresser un avertissement à la défenderesse.

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 (APD) 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 judiciaire[15]. La requête interlocutoire doit être déposée au greffe de la Cour des Marchés conformément à l'article 1034*quinquies* du C. jud.[16], 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

15° transmettre le dossier au parquet du Procureur du Roi de Bruxelles, qui l'informe des suites données au dossier ;
16° décider au cas par cas de publier ses décisions sur le site internet de l'Autorité de protection des données.

[15] 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.

[16] 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.