Chambre contentieuse

Décision quant au fond 166/2024 du 17 décembre 2024

Numéro de dossier : DOS-2021-06114

Objet : Mesures de sécurité mises en place par un hôpital

La Chambre contentieuse de l'Autorité de Protection des Données (ci-après « APD »), constituée de Monsieur Hielke HIJMANS, président, et de Messieurs Romain Robert et Jelle Stassijns, membres;

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

Vu la Loi du 3 décembre 2017 portant création de l'Autorité de protection des données[1] (ci-après « LCA ») ;

Vu le Règlement d'Ordre Intérieur (ci-après « ROI »)[2] 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 défenderesse : Y, représentée par Maîtres Victoria Ruelle et Fanny Cotton, ci-après « la défenderesse ».

[1] L'APD rappelle que la Loi cadre révisée est entrée en vigueur le 01/06/2024. Elle ne s'applique qu'aux plaintes, aux dossiers de médiation, aux requêtes, aux inspections et aux procédures devant la Chambre contentieuse initié(e)s à partir de cette date. Les dossiers initiés avant le 01/06/2024, tel que le présent dossier, sont soumis aux dispositions de l'ancienne version de la LCA accessible ici : https://www.autoriteprotectiondonnees.be/publications/loi-organique-de-l-apd.pdf

[2] L'APD rappelle que le nouveau règlement d'ordre intérieur est entré en vigueur le 01/06/2024. Il ne s'applique qu'aux plaintes, aux dossiers de médiation, aux requêtes, aux inspections et aux procédures devant la Chambre contentieuse initié(e)s à partir de cette date. Les dossiers initiés avant le 01/06/2024, tel que le présent dossier, sont soumis aux dispositions de l'ancienne version du ROI accessible ici : https://www.autoriteprotectiondonnees.be/publications/reglement-d-ordre-interieur.pdf

I. Faits et procédure

1. La défenderesse est une structure hospitalière établie en Belgique. Le [date] 2021, la défenderesse a notifié à l'APD une violation de données avec demande de rançon (« ransomware ») s'étant produite entre le 16 et le[date] 2021. Le [date] 2021, la défenderesse a procédé à une notification complémentaire au sujet de cette violation de données.

2. Le 20 octobre 2021, constatant qu'il existait des indices sérieux de l'existence d'une pratique susceptible de donner lieu à une violation des principes fondamentaux de la protection des données à caractère personnel, le Comité de direction a procédé à la saisine du Service d'inspection, en vertu de l'article 63, 1° de la LCA.

3. Le 22 novembre 2021, le Service d'inspection a formulé une demande d'informations auprès de la défenderesse dans le cadre d'une enquête d'inspection concernant la violation de données. Le 22 décembre 2021, la défenderesse a présenté ses réponses à cette demande d'informations.

4. Le 11 février 2022, le Service d'inspection a formulé une demande d'informations additionnelles dans le cadre de cette enquête d'inspection, notamment afin de mieux apprécier les mesures techniques et organisationnelles mises en œuvre par la défenderesse. Le 10 mars 2022, la défenderesse a présenté ses réponses à la demande d'informations additionnelles.

5. Le 28 avril 2022, le Service d'inspection a produit un rapport d'enquête technologique. Le 20 juin 2022, le Service d'inspection a clôturé l'enquête et a transmis le dossier au président de la Chambre contentieuse conformément à l'article 91, § 1er et § 2 de la LCA.

6. Le rapport comporte des constatations relatives à la violation de données. En particulier, le Service d'inspection en conclut que si la violation de données est incontestable suite à l'intrusion externe sur l'infrastructure de la défenderesse, son étendue demeure incertaine.

7. Le rapport d'enquête comporte également des constatations concernant l'absence de la réalisation d'une d'analyse d'impact relative à la protection des données, et l'insuffisance des mesures techniques et organisationnelles mises en place par la défenderesse. Le Service d'inspection constate, dans les grandes lignes :

   a. **Constatation 1** : Violation de l'article **35.3** du RGPD en raison de l'absence d'une analyse d'impact relative à la protection des données (ci-après « AIPD »);

b. **Constatation 2** : Violation des articles **5.1.f et 32** du RGPD en raison de l'inexistence d'une politique de sécurité de l'information effective et formelle au moment de la violation de données ;

c. **Constatation 3** : Violation des articles **5.1.f, 24 et 32** du RGPD en raison de l'inefficacité de la politique et/ou procédure de mise à jour de sécurité des équipements informatiques (logiciels) ;

d. **Constatation 4** : Violation des articles **5.1.f, 24 et 32** du RGPD en raison d'autres mesures de sécurité manquantes, à savoir :

i. l'absence d'un véritable programme de formation/sensibilisation des employés ;

ii. l'absence d'un système de préservation des logs en vue d'analyses ultérieures lors d'incidents ;

iii. l'absence de recours à des audits systématiques de la qualité de la sécurité des données à caractère personnel ; et

iv. la faible sécurisation du mot de passe d'accès au dossier informatisé du patient.

8. Le 27 septembre 2022 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. Le même jour, la défenderesse est informée par envoi recommandé des dispositions telles que reprises à l'article 95, § 2 ainsi qu'à l'article 98 de la LCA. Elle est également informée, en vertu de l'article 99 de la LCA, du délai pour transmettre ses conclusions. La date limite pour la réception des conclusions en réponse de la défenderesse a été fixée au 8 novembre 2022. La défenderesse a sollicité une demande de prolongation du délai de soumission des conclusions, laquelle lui a été accordée le 14 octobre 2022.

9. Le 8 octobre 2022, la défenderesse demande par courriel une copie du dossier (art. 95, §2, 3° LCA), laquelle lui est transmise par voie électronique le 14 octobre 2022.

10. Le 22 novembre 2022, la Chambre contentieuse reçoit les conclusions en réponse de la défenderesse. En résumé, la défenderesse présente les moyens de défense qui suivent :

- **Sur la procédure** :

a. L'irrégularité de la saisine du Comité de direction par le Secrétariat général.

b. L'absence de validité du procès-verbal du Comité de direction.

c. Le caractère erroné des indices sérieux retenus par le Comité de direction.

d. L'impossibilité d'une transmission du formulaire de notification au sein des départements de l'APD.

- **Sur le fond** :

a. **Constatation 1** : La défenderesse soutient qu'une analyse d'impact a été réalisée.

b. **Constatation 2** : La défenderesse soutient que la politique de sécurité de l'information de l'hôpital doit être comprise comme un élément parmi un ensemble de documents et de procédures mis en place, lesquels constituent les mesures organisationnelles et techniques de l'hôpital.

c. **Constatation 3** : La défenderesse soutient que la politique de mise à jour de sécurité des équipements informatiques est constituée des contrats de consultance conclus par l'hôpital afin d'assurer un contrôle mensuel de ses installations, et vise plusieurs mesures ayant été mises en place par l'hôpital postérieurement à la violation de données.

d. **Constatation 4** : La défenderesse soutient que l'ensemble des mesures prétendues manquantes a été mis en place.

11. Dans ses conclusions, la défenderesse manifeste son intention de recourir à la possibilité d'être entendue, conformément à l'article 98 de la LCA.

12. Le 20 juin 2024, les parties sont informées du fait que l'audition aura lieu le 4 juillet 2024.

13. Le 4 juillet 2024, les parties sont entendues par la Chambre contentieuse.

14. Le 22 juillet 2024, le procès-verbal de l'audition est soumis aux parties.

15. Le 29 juillet 2024, la Chambre contentieuse reçoit les remarques de la défenderesse relatives au procès-verbal.

16. Le 13 août 2024, la Chambre contentieuse fait connaître à la défenderesse son intention de procéder à l'imposition d'une amende administrative ainsi que son montant, afin de donner à la défenderesse l'occasion de présenter ses arguments à cet égard.

17. Le 3 septembre 2024, 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 que l'hôpital doit être considéré comme une « autorité publique » au sens de l'article 5[3] de la loi relative à la protection des personnes

[3] L'article 5 de la Loi cadre, prévoit que : « Pour l'application de la présente loi, on entend par "autorité publique" :
1° l'état fédéral, les entités fédérées et les autorités locales;

physiques à l'égard des traitements de données à caractère personnel du 30 juillet 2018 (ci-après « Loi cadre »), de sorte qu'il n'est pas possible de lui infliger une amende[4]. En outre, si l'hôpital devait être considéré comme personne morale à laquelle il est possible d'infliger une amende, il conteste tant le principe d'imposer une amende que son montant, tel qu'établi par la Chambre contentieuse dans le formulaire de sanction. Il fait valoir des arguments quant à la gravité faible de l'infraction et aux capacités financières limitées de l'hôpital.

II. Motivation

II.1. Mise en contexte[5]

18. Le [date] 2021, la défenderesse a notifié à l'APD une violation de données de type « ransomware » s'étant produite entre le [..] et le[date] 2021. Le [date] 2021, la défenderesse a procédé à une notification complémentaire au sujet de cette violation de données.

19. Le[date] 2021, la défenderesse a également publié un communiqué de presse pour informer le public qu'une cyberattaque avait eu lieu. Elle y explique que ses serveurs ont été touchés, paralysant une partie du système informatique.

20. Les notifications initiale et complémentaire de la violation de données indiquaient que de nombreuses catégories de données personnelles avaient été compromises, y compris des catégories particulières de données personnelles (telles que des données de santé), et des données de communications électroniques. En outre, la notification complémentaire confirmait que le nombre maximal de personnes concernées par la violation était de 300.000 personnes et que le niveau de risque pour les droits et libertés des personnes concernées était « élevé ».

2° les personnes morales de droit public qui dépendent de l'Etat fédéral, des entités fédérées ou des autorités locales;

3° les personnes, quelles que soient leur forme et leur nature qui :

- ont été créées pour satisfaire spécifiquement des besoins d'intérêt général ayant un caractère autre qu'industriel ou commercial; et

- sont dotées de la personnalité juridique; et

- dont soit l'activité est financée majoritairement par les autorités publiques ou organismes mentionnés au 1° ou 2°, soit la gestion est soumise à un contrôle de ces autorités ou organismes, soit plus de la moitié des membres de l'organe d'administration, de direction ou de surveillance sont désignés par ces autorités ou organismes;

4° les associations formées par une ou plusieurs autorités publiques visées au 1°, 2° ou 3° ».

[4] L'article 221§2 de la Loi cadre prévoit que : « L'article 83 du Règlement ne s'applique pas aux autorités publiques et leurs préposés ou mandataires sauf s'il s'agit de personnes morales de droit public qui offrent des biens ou des services sur un marché ».

[5] Les faits tels que présentés dans cette section sont fondés sur les conclusions de la défense et le rapport du Service d'inspection. Ils ne sont pas contestés par la défenderesse.

21. Il ressort de l'enquête du Service d'inspection que l'intrusion a été commise par un pirate informatique à partir de serveurs se trouvant sur le continent asiatique, via le serveur de messagerie électronique Microsoft Exchange. Le pirate a désinstallé l'antivirus et, par la suite, installé un programme malveillant. De cette manière, il a pu se créer un compte avec des accès « administrateurs ».

22. Le pirate informatique a ensuite activé BitLocker, bloquant tout accès aux données des serveurs Windows de l'Hôpital. Lorsqu'une personne tentait de s'y connecter, l'accès était donc refusé, et une demande de rançon s'affichait. Le pirate a, en outre, modifié les mots de passe des serveurs informatiques Windows pour en empêcher l'accès. L'équivalent de 5 gigas d'information ont été exportés par le pirate informatique lors de l'attaque.

23. Pendant l'attaque, les liaisons du réseau vers l'extérieur ont été coupées. Le Plan d'Urgence Hospitalier (ci-après « PUH ») a été déclenché afin de permettre la continuité de la prise en charge des patients à l'exception des urgences de l'hôpital, qui ont été fermées pendant 3 jours, mais pour lesquelles les mesures du PUH permettaient de rediriger les patients vers d'autres services d'urgence d'établissements tiers.

24. Dans ses réponses aux questions du Service d'inspection, l'hôpital confirme qu'au 20 septembre 2021, soit 3 jours après la violation de données, le logiciel qui permet l'accès au dossier patient est opérationnel à 95 %. Le [date] 2021, soit 12 jours après la violation de données, les messageries électroniques du personnel sont de nouveau opérationnelles et l'hôpital considère avoir remédié en grande partie aux conséquences de l'attaque.

25. Il s'agit de la seconde violation de données de type « ransomware » subie par l'hôpital en deux ans et demi, la première ayant eu lieu le [date] 2019. Cette première violation avait été régulièrement notifiée à l'APD.

II.2. Sur la procédure

II.2.1. Saisine du Comité de direction par le Secrétariat général :

26. **La défenderesse** défend dans ses conclusions que le Secrétariat général de l'APD n'est pas compétent pour traiter les notifications de violations de données en vertu des articles 19 et 20 de la LCA. Par conséquent, la compétence du Secrétariat général pour analyser les notifications de violation de données, puis rédiger une note à l'attention du Comité de direction n'est pas établie. En tout état de cause, ladite note aurait dû être envoyée au moins une semaine avant la séance du Comité de direction conformément à l'article 4 du ROI, or, la note du Secrétariat général n'est pas datée.

27. **La Chambre contentieuse** rappelle que l'article 4 du ROI prévoit que « Pour tous les cas nécessitant une décision stratégique du comité de direction, une proposition est élaborée par le directeur compétent par le biais d'une note. Sauf en cas de nécessité urgente, le dossier sera mis à la disposition des membres au moins une semaine avant la séance, le cas échéant avec les annexes requises. Lors de la séance, le dossier sera expliqué par le directeur compétent ».

28. Le RGPD prévoit, en son article 33§1, que « 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 (…) » sans distinction du département ou service compétent de l'autorité pour traiter ladite violation. La Chambre contentieuse note que ni la LCA, ni le ROI, n'attribuent à un département de l'APD la compétence exclusive pour traiter les notifications de violation de données personnelles. Contrairement à ce que soutient la défenderesse pendant l'audition, il n'existe pas de vide juridique sur ce point, dans la mesure où le RGPD prévoit qu'une telle compétence revient aux autorités de contrôle. Si, comme en l'espèce, la loi nationale ne prévoit rien, il n'en incombe pas moins à chaque autorité de mener à bien les missions qui lui sont conférées par le RGPD, et ce pour donner un effet utile au texte[6].

29. Le Secrétariat général, dont l'une des tâches exécutives est de formuler des avis dans le cadre des AIPD (article 20§1, 3° de la LCA), dispose de l'expérience nécessaire pour apprécier les risques liés aux traitements de données mis en place par les responsables de traitement. Par ailleurs, il a pour tâche exécutive de surveiller les développements technologiques qui ont un impact sur la protection des données personnelles (article 20§1, 3° de la LCA), ce qui nécessite un suivi des technologies utilisées par les pirates informatiques, lesquelles peuvent être décrites dans les formulaires de notification de violation de données.

30. De fait, le Secrétariat général est un département de l'APD disposant d'une expertise privilégiée pour analyser les risques découlant d'une violation de données notifiée à l'APD.

31. D'autre part, le directeur du Secrétariat général a la compétence, comme tout autre directeur, de présenter un dossier au Comité de direction pour examen en vue d'une éventuelle activation de l'article 63.1° de la LCA. Compte tenu des développements qui précèdent (paragraphes 29 et 30), il ressort que le directeur du Secrétariat général était compétent, sans exclure que d'autres directeurs aient pu faire de même, pour

[6] Voir sur ce point les missions conférées aux autorités de contrôle par l'art. 57.1 du RGPD.

proposer une note au Comité de direction, sur la base de son analyse du formulaire de notification de violation de données, au sens de l'article 4 du ROI.

32. Par ailleurs, la Chambre contentieuse observe que si l'article 4 du ROI impose au directeur compétent de remettre le dossier aux membres du Comité de direction au moins une semaine avant la séance, le ROI n'impose pas au directeur d'apposer une date sur la note elle-même. En l'espèce, l'APD a proposé à la défenderesse de constater avant l'audition que cette disposition du ROI avait été observée, puisque la note a été envoyée par e-mail une semaine avant la séance du Comité de direction. La défenderesse n'a pas contesté cette date pendant l'audition.

33. En tout état de cause, cette disposition relève des règles d'organisation internes à l'APD et ne peut entraîner la nullité de la procédure, comme le soutient la défenderesse. Ce délai d'ordre, qui est un délai fixé à titre indicatif et non impératif, vise à protéger les directeurs dans leurs fonctions et non à conférer des droits aux parties à une procédure. Par conséquent, ce délai n'a aucun effet vis-à-vis des tiers et ne peut être invoqué par la défenderesse pour demander l'annulation de la présente procédure. Il convient par ailleurs de rappeler que ce délai a été respecté.

34. **En conclusion, le directeur du Secrétariat général a valablement respecté la procédure prescrite à l'article 4 du ROI en rédigeant une note au Comité de direction. Cette note a été remise aux membres du Comité de direction au moins une semaine avant la séance. Les arguments de la défenderesse sont dès lors infondés.**

II.2.2. Procès-verbal du Comité de direction :

35. **La défenderesse** explique qu'il existe des doutes quant au fait qu'un procès-verbal de la décision du Comité de direction ait été dressé et signé par le président du Comité de direction, ce qui constitue une violation de l'article 16 de la LCA. En outre, elle considère qu'il n'est pas démontré que la majorité des membres du Comité de direction étaient présents, ni qu'une majorité des membres ait voté favorablement en vertu de l'article 3 du ROI. La défenderesse soutient qu'il n'est par ailleurs pas établi que le président de la Chambre contentieuse se soit abstenu de participer au vote du Comité de direction sur ce point, dès lors qu'il est susceptible par la suite de devoir prendre position au fond.

36. **La Chambre contentieuse** rappelle que les procès-verbaux du Comité de direction couvrent de nombreux thèmes, y compris des décisions stratégiques de l'APD et qu'ils contiennent des données personnelles. Conformément au principe de minimisation des données (article 5.1.c du RGPD), et au respect du principe de

confidentialité s'appliquant aux membres du Comité de direction (art. 48 LCA), les membres ne transmettent pas leurs procès-verbaux dans leur intégralité aux parties concernées par une procédure, mais seulement un extrait dudit procès-verbal afin de permettre aux parties à une procédure d'apprécier son existence pour la section qui les concerne.

37. Dans le cas où une partie redoute le non-respect d'une formalité, l'APD est disposée à transmettre les informations supplémentaires souhaitées par une partie, afin de lui permettre d'apprécier le respect des formalités contestées. Une telle possibilité a été offerte à la défenderesse avant l'audition, afin de lui permettre de constater le respect par l'APD des formalités qu'elle soulevait à peine de nullité de la procédure.

38. La défenderesse a pu constater sur le procès-verbal que l'ensemble des membres du Comité de direction étaient présents lors de la délibération, qu'aucune objection de la part d'un des membres du Comité de direction n'est annotée et que le procès-verbal a bien été signé par le Président du Comité de direction. Elle a également pu constater que le Comité de direction a décidé de saisir le Service d'inspection sur la base de l'article 63.1° de la LCA. L'argument de la défenderesse tendant à contester l'existence d'un procès-verbal et le respect de son formalisme n'est donc pas valable.

39. Conformément à une jurisprudence constante, la critique de la partialité ne peut se fonder sur une situation découlant de l'application normale de la loi (voir en ce sens l'arrêt du Conseil d'État du 11 mai 2021[7]). Or, le Comité de direction est composé du président de la Chambre contentieuse (article 12 LCA). Le Comité de direction est également compétent pour saisir le Service d'inspection en cas de constatation d'indices sérieux de l'existence d'une pratique susceptible de violer les principes fondamentaux de la protection des données personnelles (article 63.1° de la LCA).

40. Aucun article de la LCA ne prévoit d'exception relative à la participation du président de la Chambre contentieuse aux décisions prises par le Comité de direction. Lorsque le président de la Chambre contentieuse est exclu d'un rôle ou d'une position, la loi le prévoit explicitement (voir les articles 13 et 18 de la LCA), preuve que le législateur n'a pas entendu vouloir écarter le président de la Chambre contentieuse de la participation aux délibérations du Comité de direction. Celui-ci est donc compétent pour participer aux délibérations du Comité de direction (art. 16 de la LCA) et pour prendre une décision sur le fond (art. 98 et suivants de la LCA).

---

[7] Voir l'arrêt du Conseil d'Etat du 11 mai 2021, n°250.571 disponible sur le lien suivant : http://www.raadvst-consetat.be/Arrets/250000/500/250571.pdf#xml=http://www.raadvst-consetat.be/apps/dtsearch/getpdf.asp?DocId=39004&Index=c%3a%5csoftware%5cdtsearch%5cindex%5carrets%5ffr%5c&HitCount=2&hits=16+17+&083572024517

41. La Chambre contentieuse rappelle qu'en l'espèce, elle siège collégialement, c'est-à-dire à trois membres. Elle rappelle que le Comité de direction a également siégé à cinq membres au moment de sa délibération concernant la présente procédure. Dans de telles situations de collégialité, la Cour des marchés rappelle que quand bien même la partialité d'un membre serait démontrée, elle ne permet pas d'affecter à elle seule la légalité de la décision attaquée[8].

42. Enfin, la prétendue partialité d'un organe collégial doit être concrètement démontrée, ce qui suppose de mettre en évidence des faits ou des comportements précis qui concernent cet organe, et donc posés par ses membres[9]. S'agissant des membres du Comité de direction et de la Chambre contentieuse, l'article 43§2 de la LCA prévoit explicitement que : « Il leur est interdit d'être présents lors d'une délibération ou décision sur les dossiers pour lesquels ils ont un intérêt personnel ou direct ou pour lesquels leurs parents ou alliés jusqu'au troisième degré ont un intérêt personnel ou direct ». Ces situations de partialité sont prévues par la loi.

43. S'il est vrai que le législateur n'a pas prévu de régime de récusation particulier pour garantir l'indépendance et l'impartialité des membres de la Chambre contentieuse[10], la Chambre contentieuse est disposée à répondre aux arguments sérieux présentés par des parties concernant la partialité de ces membres. En l'espèce, la défenderesse ne rapporte pas d'indices de partialité de la part du président de la Chambre contentieuse, qui auraient pu justifier sa récusation.

44. **En conclusion, ni la validité du procès-verbal du Comité de direction, ni la participation du président de la Chambre contentieuse à la délibération ne peuvent être contestées. La procédure a respecté les exigences légales, et aucune preuve de partialité n'a été apportée.**

II.2.3. Indices sérieux retenus par le Comité de direction :

45. **La défenderesse** soutient que les indices retenus par le Comité de direction pour constater qu'il existait des indices sérieux de l'existence d'une pratique susceptible de donner lieu à une violation des principes fondamentaux de la protection des données à caractère personnel sont erronés. Elle conteste que la motivation du

[8] Cour d'appel de Bruxelles, Section Cour des marchés, 19ème Chambre A, arrêt du 7 décembre 2022, disponible sur le lien suivant : https://www.gegevensbeschermingsautoriteit.be/publications/arrest-van-7-december-2022-van-het-marktenhof-ar-556-beschikbaar-in-het-frans.pdf

[9] Cour d'appel de Bruxelles, Section Cour des marchés, 19ème Chambre A, Cour des Marchés, arrêt du 7 décembre 2022, disponible sur le lien suivant : https://www.gegevensbeschermingsautoriteit.be/publications/arrest-van-7-december-2022-van-het-marktenhof-ar-556-beschikbaar-in-het-frans.pdf

[10] Cour des marchés, arrêt du 31 octobre 2023, n°2023/AR/821

Comité de direction soit établie par référence à la note du Secrétariat général. Enfin, elle explique que le fait que l'hôpital ait été victime d'une attaque informatique ne découle pas d'un manquement de sa part et ne constitue pas un indice sérieux au sens de l'article 63.1° de la LCA.

46. **La Chambre contentieuse** rappelle qu'en vertu des pouvoirs conférés au Comité de direction, il lui appartient de constater si des indices sérieux révèlent l'existence de pratiques pouvant donner lieu à une violation des principes fondamentaux de la protection des données (article 63.1° de la LCA). Comme l'a rappelé la Cour des marchés, il s'agit là d'une compétence discrétionnaire de l'APD[11].

47. Le Conseil d'état accepte la motivation par référence, pour autant que la pièce à laquelle il est fait référence fasse partie du dossier, ce qui est le cas en l'espèce (arrêt du Conseil d'état du 7 mai 2013, n°223.440). En effet, la décision du Comité de direction fait référence à la note qui lui a été fournie, et se fonde sur celle-ci pour retenir les indices suivants :

    a. L'arrêt du réseau informatique de l'hôpital, qui a entraîné l'annulation d'opérations et de consultations prévues ainsi que la fermeture des urgences.

    b. Le degré de sensibilité des données comprises dans la violation, incluant notamment le numéro national, le numéro d'identification de la sécurité sociale, des données génétiques, biométriques, des données relatives à la santé, aux soins, à la vie sexuelle ou à l'orientation sexuelle, des condamnations pénales, des extraits du casier judiciaire, le contenu de communications électroniques et des données financières.

    c. L'indication dans le formulaire de l'impact possible de la violation de données sur les droits et libertés des personnes concernées, telle que l'indisponibilité des données ou des traitements empêchant la poursuite de la fourniture du service attendu.

    d. Le grand nombre de personnes touchées, soit potentiellement 300 000 personnes.

    e. L'existence d'une précédente violation de données importante de type « ransomware » en date du [date] 2019. Sur ce point, la défenderesse a confirmé qu'aucune rançon n'avait été versée.

[11] Cour d'appel de Bruxelles, Section Cour des marchés, 19ème Chambre A, Cour des Marchés, arrêt du 22 février 2022, disponible sur le lien suivant : https://www.autoriteprotectiondonnees.be/publications/arret-du-22-fevrier-2023-de-la-cour-des-marches-ar-953.pdf, p. 40 et s.

48. Ces informations étaient basées sur la description de la violation de données, telle que décrite dans les formulaires de notifications initiale et complémentaire transmis à l'APD par l'hôpital. Ce n'est qu'à travers l'enquête menée ultérieurement par le Service d'inspection que ce dernier a permis de relativiser dans une certaine mesure l'étendue de cette violation et de la précédente violation de 2019.

49. Cependant, l'enquête n'a pas permis de faire toute la lumière sur les circonstances exactes de la violation (voir paragraphe 106 et suivants s'agissant de la préservation des logs). En tout état de cause, si des informations erronées ont été communiquées à l'APD par le biais de ces notifications, il ne peut être reproché au Comité de direction de s'en être servi pour caractériser des indices sérieux justifiant l'ouverture d'une enquête. À l'époque de la décision du Comité de direction et sur la base des éléments dont celui-ci disposait à la lecture de la notification initiale, le Comité de direction a constaté souverainement qu'il existait des indices sérieux justifiant l'ouverture d'une enquête. La Chambre contentieuse ne peut exercer de contrôle sur la décision du Comité de direction à cet égard autre qu'un contrôle marginal. Or, le Comité de direction n'a pas, en appréciant le caractère sérieux des indices en question, excédé ses compétences dans le cas d'espèce.

50. Par ailleurs, la défenderesse conteste que le Comité de direction ait tenu compte d'une précédente violation de données survenue en 2019 par le même hôpital. Cependant, le Comité de direction était en droit de se fonder sur les informations mises à la disposition de l'APD à travers les formulaires de notification de violation de données reçus de l'hôpital. Ces formulaires constituent une source essentielle et légitime d'information pour l'APD, permettant de caractériser des indices sérieux de potentielles violations de la législation relative à la protection des données. La récurrence de violations de données au sein d'une même institution, en particulier lorsqu'elles surviennent à des intervalles rapprochés et impliquent des risques élevés pour les droits et libertés des personnes concernées, renforce raisonnablement la présence d'indices sérieux au sens de l'article 63.1° de la LCA.

51. Le Comité de direction a estimé souverainement que le fait qu'un hôpital subisse deux violations de données, présentant chacune des risques « élevés » pour les droits et libertés des personnes concernées, et ce en l'espace de deux ans, constituait un indice sérieux additionnel révélant l'existence de pratiques pouvant donner lieu à une violation des principes fondamentaux de la protection des données.

52. En outre, la défenderesse semble confondre la notion d'« indices sérieux » avec le constat d'une violation du RGPD. Le Comité de direction ne dispose pas du pouvoir de constater une violation du RGPD, et une telle constatation n'est pas requise pour qu'il puisse faire usage de l'article 63.1° de la LCA. La compétence d'établir une violation

du RGPD est réservée à la Chambre contentieuse. Ce n'est que lorsqu'elle dispose d'un dossier en état, qui contient des conclusions des parties et un éventuel rapport d'enquête, que la Chambre contentieuse peut déterminer si une attaque informatique constitue une violation du RGPD[12]. Au moment de l'activation de l'article 63.1°, seul l'existence d'indices sérieux est nécessaire, ce qui a été apprécié souverainement (voir les paragraphes 49 à 51 ci-dessus).

53. **En conclusion, le Comité de direction était fondé à constater la suffisance du caractère sérieux des indices en cause, sur la base des informations transmises par la défenderesse (article 63.1° de la LCA).**

II.2.4. Transmission du formulaire de notification au sein des départements de l'APD :

54. **La défenderesse** considère que le formulaire de notification de la violation de données n'a pas à être partagé au sein des départements de l'APD, pour cause d'absence de disposition légale prévue à cet effet. En outre, elle soutient que ni le RGPD ni la LCA ne prévoient la possibilité pour une notification de violation de données de déboucher sur une procédure devant la Chambre contentieuse. Enfin, elle prétend que le Comité Européen de Protection des Données (ci-après « CEPD ») ne prévoit pas qu'une telle notification soit utilisée pour justifier la saisine du Service d'inspection et reprocher au déclarant d'autres manquements.

55. **La Chambre contentieuse** conteste les arguments soulevés dans les conclusions de la défense, et rappelle que le RGPD prévoit, en son article 33§1, que « 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 (…) ». Par ailleurs, « Une telle notification peut amener une autorité de contrôle à intervenir conformément à ses missions et à ses pouvoirs fixés par le présent règlement » (considérant 87 du RGPD).

56. Dès lors, toute autorité de contrôle est légalement habilitée à connaître du contenu d'un formulaire de notification de violation de données qui lui est notifié. Contrairement aux affirmations soulevées en défense, le RGPD prévoit bien qu'une telle notification puisse amener une autorité à faire usage de ses pouvoirs d'enquête et de poursuite. Considérant la structure de l'APD, cette circonstance justifie forcément la possibilité d'une transmission du formulaire entre ses services compétents.

---

[12] Chambre contentieuse, décision quant au fond 170/2023 du 20 décembre 2023, disponible sur le lien suivant : https://www.autoriteprotectiondonnees.be/publications/decision-quant-au-fond-n-170-2023.pdf

57. Quand bien même la défenderesse considérerait que le considérant 87 du RGPD n'est pas suffisamment explicite, la Chambre contentieuse rappelle que lorsqu'une disposition de droit de l'Union Européenne (« UE ») est susceptible de plusieurs interprétations, il faut donner la priorité à celle qui est de nature à sauvegarder son effet utile, selon les principes généraux du droit de l'UE[13]. L'interprétation du droit de l'UE doit être faite de manière à garantir l'efficacité du système juridique de l'UE et à éviter que les dispositions soient vidées de leur sens[14] L'argument de la défenderesse selon lequel l'APD n'avait pas à transmettre le formulaire de notification de violation de données entre les départements impliqués dans le suivi de la présente affaire n'est dès lors pas fondé.

58. Enfin, contrairement aux allégations de la défenderesse, les lignes directrices du CEPD sur le calcul des amendes administratives au titre du RGPD[15] confirment la possibilité d'un usage par l'autorité de contrôle d'une notification de données qui lui a été transmise. Ces lignes directrices prévoient explicitement que lorsque l'autorité de contrôle a eu connaissance d'une violation, justifiant l'imposition d'une amende, par le biais d'une notification d'une violation de données, ce facteur doit être considéré comme neutre dans le calcul de l'amende.

59. **En conclusion, le formulaire de notification de la violation de données a valablement été partagé au sein des départements de l'APD, afin de leur permettre de faire usage de leurs pouvoirs d'enquête et de poursuite.**

II.3. Sur le fond

II.3.1. Constatation 1 : Sur l'analyse d'impact relative à la protection des données

60. *Premièrement*, **la défenderesse** soutient que le traitement relatif aux messages électroniques du personnel ayant été le seul à avoir été affecté par la violation de données, elle n'était pas soumise à l'obligation de mettre en place une AIPD pour ce traitement, lequel ne nécessite pas le traitement de données sensibles. Pendant l'audition, la Chambre contentieuse a questionné davantage la défenderesse sur son

[13] Article « Le droit de l'Union européenne devant les juridictions de l'ordre judiciaire », Jérémie Van Meerbeeck, Université Catholique de Louvain, 22 septembre 2015, paragraphe 11

[14] Voir les arrêts de la CJCE (prédécesseur de la CJUE), 4 déc. 1974, Van Duyn, aff. 41/74 et 3 avr. 2008, Endendijk, aff. C-187/07, pts 14-26.

[15] Voir sur ce point le paragraphe 98 des lignes directrices 04/2022 du CEPD sur le calcul des amendes administratives au titre du RGPD, qui reprennent sur ce point une position établie par les lignes directrices sur l'application et la fixation des amendes administratives WP253, approuvées par le CEPD au cours de sa première réunion plénière du 25 mai 2018, accessibles au lien suivant :https://www.edpb.europa.eu/system/files/2024-01/edpb_guidelines_042022_calculationofadministrativefines_fr_0.pdf

raisonnement consistant à affirmer l'absence de traitement de données sensibles dans le cadre du traitement des messages électroniques du personnel hospitalier. La défenderesse a soutenu que des données sensibles étaient probablement échangées par messages électroniques, mais a déclaré que ces données sensibles étaient chiffrées.

61. *Deuxièmement*, elle soutient que la réalisation d'une AIPD ne doit pas prendre de forme particulière, et qu'il est erroné de soutenir qu'aucune AIPD n'a été effectuée dans la mesure où l'hôpital a mis en place des mesures de sécurité qui sont le fruit d'analyses de risques.

62. *Troisièmement*, elle prétend que dans la mesure où le traitement a été mis en œuvre avant l'entrée en vigueur du RGPD en mai 2018, ce dernier n'est pas soumis à l'obligation de réaliser une AIPD, et que quand bien même il le serait, ce dernier aurait été exempté de cette obligation grâce au « délai de grâce » de trois ans octroyé par le CEPD.

63. *Premièrement*, **la Chambre contentieuse** rappelle qu'une AIPD est prévue dans plusieurs cas, notamment en cas de traitement à grande échelle de catégories particulières de données (article 35.3.b) du RGPD). Une AIPD doit au moins contenir (article 35.7, et considérants 84 et 90 du RGPD) :

   a. une description systématique des opérations de traitement envisagées et des finalités du traitement ;

   b. une évaluation de la nécessité et de la proportionnalité des opérations de traitement ;

   c. une évaluation des risques pour les droits et libertés des personnes concernées ;

   d. les mesures envisagées pour :

      i. faire face aux risques ;

      ii. apporter la preuve du respect du RGPD.

64. En l'espèce, le responsable de traitement traite des données sensibles (notamment des données de santé et des données génétiques) de personnes vulnérables (patients) à grande échelle (300 000 patients en base de données), ce qui lui impose de se conformer à cette obligation. La Chambre contentieuse rappelle que l'un des intérêts de réaliser une AIPD est de permettre au responsable de traitement d'identifier préventivement les failles de sécurité et d'adopter des mesures appropriées pour protéger les données personnelles contre des violations de données.

65. Contrairement aux allégations de la défenderesse, le fait que l'attaque se soit concentrée sur la messagerie électronique du personnel et non sur les dossiers médicaux des patients n'exonère pas la défenderesse de son devoir de réaliser une AIPD. La Chambre contentieuse rappelle que la définition de « traitement » au sens du RGPD est large, et inclut notamment la conservation, la collecte, la consultation, l'utilisation et la mise à disposition de données personnelles (article 4 du RGPD). Quand bien même l'attaque n'aurait visé que les messageries électroniques du personnel, le fait que ces dernières permettent de traiter des données sensibles de personnes vulnérables à grande échelle impose dès lors à la défenderesse de se conformer à son obligation de réaliser une AIPD concernant ce traitement, indépendamment de la question de savoir si ces données sont chiffrées pendant l'envoi de messages électroniques. En tout état de cause, la présente constatation ne se borne pas à examiner la réalisation d'une AIPD s'agissant du seul traitement spécifique relatif aux messageries électroniques du personnel[16].

66. En outre, il apparaît non pertinent de la part de la défenderesse de prétendre que seules les messageries électroniques du personnel ont été affectées, dans la mesure où il ressort du rapport d'enquête que les serveurs de l'hôpital ont quant à eux été paralysés (dont le logiciel supportant les dossiers médicaux), et que celui-ci a cessé d'être opérationnel du fait de l'attaque. En outre, il ressort clairement de l'enquête que des indices ont été retrouvés sur le « serveur radiologie ». Selon les conclusions de la défense : « L'Hôpital a pu progressivement mais rapidement relancer ses services sans risques, en ce compris le service de radiologie », et « Pour finir, les recherches approfondies faites par l'Hôpital et les prestataires auxquels elle a fait appel ont montré que lors de l'attaque, seuls 5 gigas d'informations ont été exportés de l'un des serveurs de l'Hôpital vers Internet. Or, le serveur en question contient l'ensemble des radiographies (…) ». Dès lors, la violation de données a bien porté sur des catégories sensibles de données personnelles, en l'occurrence les données de santé des patients de l'hôpital traitées à grande échelle.

67. *Deuxièmement*, il est inexact d'avancer que l'AIPD ne doit pas prendre de forme particulière, puisque le principe de responsabilité du RGPD impose aux responsables de traitement d'être en mesure de démontrer que leurs obligations sont respectées (art. 5.2 et 24 du RGPD) et que l'article 35.7 du RGPD énumère le contenu minimal d'une AIPD. Il en ressort que l'AIPD doit être effectuée dans un document distinct qui ne se confond pas avec d'autres éventuelles analyses de risques. Les analyses de

[16] Conformément à l'article 35.1 du RGPD, il appartient au responsable de traitement d'examiner s'il est opportun de réaliser une ou plusieurs AIPD : « Une seule et même analyse peut porter sur un ensemble d'opérations de traitement similaires qui présentent des risques élevés similaires ».

risques présentées par la défenderesse ne remplissent pas les critères nécessaires à la constatation de l'existence d'une AIPD par la Chambre contentieuse.

68. En tout état de cause, la défenderesse a confirmé dans ses réponses aux questions du Service d'inspection qu'aucune AIPD n'avait été réalisée par le responsable de traitement. Le fait que des analyses de risques aient été effectuées par les auditeurs de l'hôpital et qu'une AIPD ait été commandée ne permet pas à la Chambre contentieuse de considérer qu'une AIPD a été réalisée par la défenderesse.

69. *Troisièmement*, la défenderesse soutient à tort que dans la mesure où le traitement a été mis en œuvre avant l'entrée en vigueur du RGPD en mai 2018, ce dernier n'est pas soumis à l'obligation de réaliser une AIPD. S'agissant des traitements mis en place avant l'entrée en vigueur du RGPD, la Chambre contentieuse rappelle que le CEPD indique que « L'obligation d'effectuer une AIPD s'applique aux opérations de traitement existantes [*mises en place avant le RGPD*] susceptibles d'engendrer un risque élevé pour les droits et libertés des personnes physiques et pour lesquelles les risques associés ont évolué, compte tenu de la nature, de la portée, du contexte et des finalités du traitement » (soulignement et informations sous crochets ajoutés)[17].

70. Dans la mesure où les risques du secteur hospitalier sont en constante évolution (fait qui n'est pas contesté par la défenderesse)[18] et que les enjeux d'un blocage des activités d'un hôpital présentent un risque élevé pour les droits et libertés des personnes physiques[19], la Chambre contentieuse réfute l'argument selon lequel l'hôpital aurait été exempté de l'obligation de réaliser une AIPD.

71. Enfin, la Chambre contentieuse conteste les affirmations de la défenderesse soulevées pendant l'audition, selon lesquelles le CEPD aurait accordé un délai de grâce de 3 ans concernant la réalisation d'AIPD pour les traitements existants, suivant l'entrée en vigueur du RGPD. Si ce délai de grâce a pu être autorisé par des autorités nationales sous des conditions spécifiques, telles que la Commission Nationale de l'Informatique et des Libertés (CNIL) en France, le CEPD n'a pas octroyé de tel délai.

---

[17] Voir les lignes directrices du CEPD 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, accessibles depuis le lien suivant : https://ec.europa.eu/newsroom/article29/items/611236/en (page 16)

[18] La défenderesse soutient elle-même dans ses conclusions que les hôpitaux sont sujets à des risques spécifiques et en constante évolution : « (…) les structures hospitalières sont des cibles privilégiées pour les pirates informatiques », « Les hackers sont nombreux, disposent de ressources inépuisables et prennent tout particulièrement pour cible les groupes hospitaliers »,

[19] Comme rappelé dans les lignes directrices sur la notification de violations de données du WP29 : « Si des données médicales critiques concernant les patients d'un hôpital sont rendues indisponibles, ne serait-ce que temporairement, cela pourrait présenter un risque pour les droits et libertés des personnes concernées; des opérations pourraient par exemple être annulées et des vies mises en danger ». Ces Lignes directrices sur la notification de violations de données à caractère personnel en vertu du règlement (UE) 2016/679 ont été publiées par le WP29 (prédécesseur du CEPD). Elles sont accessibles depuis le lien suivant : https://ec.europa.eu/newsroom/article29/items/612052/en (voir page 9)

En tout état de cause, l'hôpital ne disposait toujours pas d'AIPD plus de trois ans après l'entrée en vigueur du RGPD, soit le 25 mai 2018[20]. L'argument lié à l'existence d'un prétendu délai de grâce – *quod non* – ne peut donc convaincre.

72. **En conclusion, la défenderesse a manqué à son obligation de réaliser une AIPD au sens de l'article 35.3 du RGPD.**

II.3.2. Constatation 2 : Sur la politique de sécurité de l'information effective et formelle

73. *Premièrement,* **la défenderesse** soutient que l'APD n'est pas compétente en matière de contrôle du respect de l'obligation d'application des normes minimales relatives à la sécurité de l'information et à la vie privée pour les institutions de sécurité sociale en vertu de l'article 2, alinéa 1er, 2° de la loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque Carrefour de la Sécurité Sociale (ci-après, les « Normes minimales »)[21]. *Deuxièmement*, elle soutient que le RGPD ne contient aucune obligation formelle de disposer d'une politique de sécurité de l'information, et n'impose, a fortiori, aucun formalisme pour une telle politique. Elle explique qu'en l'espèce, la politique de sécurité de l'information de l'hôpital doit être comprise comme un élément parmi un ensemble de documents et de procédures mis en place, lesquels constituent les mesures organisationnelles et techniques de l'hôpital.

74. *Premièrement*, **la Chambre contentieuse** rappelle qu'en vertu de l'article 32. 1 du RGPD, il incombe à l'APD de vérifier le respect des mesures techniques et organisationnelles appropriées, en tenant compte de « l'état des connaissances ». Les Normes minimales précitées, ayant force contraignante pour les institutions de sécurité sociale en matière de sécurité des données personnelles en Belgique, constituent une référence utile à « l'état des connaissances » à laquelle la Chambre contentieuse peut se référer. En effet, ces normes prévoient que : « Par ailleurs, il est de bon usage que ces normes s'appliquent également à la sécurité de l'information et à la vie privée au sens large du terme (…) »[22].

---

[20] La date d'entrée en vigueur du RGPD est le 25 mai 2018, tandis que l'attaque a été subie le [...] 2021, soit plus de trois ans plus tard.

[21] Les Normes minimales sécurité de l'information et vie privée, en leur version du 7 mars 2017, sont accessibles sur ce lien : https://www.ksz-bcss.fgov.be/sites/default/files/assets/protection_des_donnees/mnm_normes_minimales.pdf

[22] Voir les Normes minimales précitées, accessibles depuis le lien suivant : https://www.ksz-bcss.fgov.be/sites/default/files/assets/protection_des_donnees/mnm_normes_minimales.pdf, page 3, dont le passage complet est reproduit ci-contre : « Par ailleurs, il est de bon usage que ces normes s'appliquent également à la sécurité de l'information et à la vie privée au sens large du terme, comme prévu à l'arrêté royal du 17 mars 2013 relatif aux conseillers en sécurité institués par la loi du 15 août 2012 relative à la création et à l'organisation d'un intégrateur de services fédéral et comme repris dans l'arrêté royal du 12 août 1993 relatif à l'organisation de la sécurité de l'information dans les institutions de sécurité sociale: « stratégie, règle, procédures et moyens de protection de tout type d'information tant dans les systèmes de

75. En outre, la Chambre contentieuse constate que la politique de sécurité de l'information de 2022 de l'hôpital (voir paragraphe 78), contient une obligation de respecter les Normes minimales. Ainsi, le non-respect par la défenderesse des obligations de sécurité contenues dans ces Normes minimales constitue en soi un manquement aux mesures techniques et organisationnelles supposées être mises en place par la défenderesse. La remarque préliminaire de la défenderesse n'est dès lors pas fondée, et la Chambre contentieuse tiendra compte des Normes minimales dans ses développements.

76. *Deuxièmement*, la Chambre contentieuse rappelle que le RGPD impose au responsable de traitement de traiter les données personnelles de manière à garantir une sécurité appropriée, à l'aide de mesures techniques ou organisationnelles adaptées (article 5§1.f) du RGPD), ci-après dénommés « principes d'intégrité et de confidentialité ». L'article 32 du RGPD contient davantage de précisions sur ces mesures techniques et organisationnelles, par exemple, l'obligation du responsable de traitement de s'assurer que ces mesures garantissent un niveau de sécurité adapté au risque. En outre, l'article 5.2 du RGPD prévoit que « Le responsable du traitement est responsable du respect du paragraphe 1 et est en mesure de démontrer que celui-ci est respecté ». Ce principe est appelé le principe de responsabilité.

77. Elle note que la défenderesse lui a transmis de nombreux documents censés établir, pris dans leur ensemble, l'existence d'une politique de sécurité de l'information de l'hôpital (par exemple, le règlement de travail du personnel de l'hôpital, le PUH, etc.).

78. **La politique de sécurité de l'information du 3 mars 2022** : La Chambre contentieuse prend note de la transmission de la politique de sécurité de l'information susvisée, dont la première version est celle du 3 mars 2022. Pendant l'audition, la défenderesse a confirmé qu'avant cette date, la politique de sécurité de l'information était composée d'un ensemble de documents (voir paragraphe 84). Or, la mise en place d'un ensemble de documents sans lien entre eux, ni référence les uns aux autres, avec des finalités étrangères à la mise en place de mesures techniques et organisationnelles prévues par le RGPD, ne constitue pas des « mesures techniques et organisationnelles appropriées » permettant de faire face aux risques, au sens de l'article 32.1 du RGPD. En outre, les Normes minimales auxquelles la politique de sécurité de l'information de 2022 fait référence, imposent de disposer d'une politique formelle : « Toute organisation doit disposer d'une politique de sécurité de

transmission que dans les systèmes de traitement en vue de garantir la confidentialité, la disponibilité, l'intégrité, la fiabilité, l'authenticité et l'irréfutabilité de l'information ».

l'information formelle et actualisée, approuvée par le responsable de la gestion journalière » (soulignement ajouté).

79. La Chambre contentieuse relève que cette politique à caractère très général, contient elle-même la mention qu'il s'agit d'un « document de base ». Ce document de base impose de « Mettre au point une politique claire et précise relative à la sécurité de l'information et de la vie privée, la valider, la communiquer et l'actualiser afin de garantir la disponibilité, l'intégrité, et la confidentialité en adéquation avec les objectifs de la Y ».

80. La Chambre contentieuse note en outre que ce document de base a été mis en place postérieurement à la violation de données et qu'il ne saurait être considéré par la Chambre contentieuse comme permettant de justifier l'existence d'une telle politique au moment de la violation de données. De plus, il ne constitue pas un document exhaustif ou final, dans le sens où il renvoie à d'autres documents le soin de clarifier son application. Ce document de base ne suffit pas à lui seul pour répondre pleinement aux exigences de mise en place de mesures organisationnelles appropriées au sens de l'article 32.1 du RGPD, et a de plus été mis en place postérieurement à la violation.

81. **La politique claire et précise relative à la sécurité de l'information et de la vie privée :** La défenderesse a confirmé pendant l'audition que la politique « claire et précise » relative à la sécurité de l'information, qu'il lui appartenait de mettre en place selon le document de base précité, n'a pas été mise en place. Elle maintient en outre que sa politique de sécurité demeure constituée d'un ensemble de documents (voir paragraphe 84).

82. La Chambre contentieuse constate que l'objet de cette politique claire et précise était d'entrer dans les détails de la mise en œuvre des mesures techniques et organisationnelles de la défenderesse. En effet, la politique de sécurité de l'information du 3 mars 2022 énonce que : « Les paragraphes suivants présentent, sans entrer dans les détails de la mise en œuvre, les principales mesures de gestion encadrant le management de la sécurité de l'information de la Y. ». La Chambre contentieuse constate qu'elle n'est pas en mesure d'apprécier pleinement les mesures techniques et organisationnelles mises en œuvre en adéquation avec les objectifs de la Y, du fait de l'absence de cette politique claire et précise.

83. La Chambre contentieuse ne considère pas que la mise en place d'un ensemble de documents tels que décrits au paragraphe 77 permet de remplir la condition de mettre en place des « mesures techniques et organisationnelles appropriées ». La mise en place d'une « politique claire et précise » aurait permis de remplir cette condition, *quod non*. Elle constate dès lors un manquement à l'article 32.1 du RGPD.

84. **L'ensemble de documents transmis par la défenderesse :** La majorité des documents transmis ont été mis en place postérieurement à la seconde violation de données. Leur utilité dans le cadre de la présente procédure est donc limitée à l'influence que cette mise en place tardive aurait concernant l'établissement d'une éventuelle sanction, en particulier l'évaluation du montant d'une amende potentielle. Ils ne permettent pas à la Chambre contentieuse d'apprécier le niveau de conformité de la défenderesse, ni aux principes d'intégrité et de confidentialité, ni aux exigences de sécurité du RGPD, au moment de la seconde violation de données.

85. S'agissant des documents officiels dont la date permet de démontrer qu'ils étaient mis en place au moment de la seconde violation, la Chambre contentieuse relève qu'aucun de ces documents n'a vocation à démontrer la conformité par l'hôpital aux articles 5.1.f) et 32 du RGPD. L'APD rappelle à cet égard que le responsable du traitement doit être en mesure de démontrer que les principes exposés à l'article 5.1 du RGPD sont respectés.

86. A titre d'exemple, le PUH a pour objet de définir les procédures pour une prise en charge efficace de l'afflux soudain de patients sans que cela ne mette en péril les soins administrés aux patients déjà hospitalisés. La charte informatique du personnel est une mesure contractuelle permettant au responsable de traitement d'imposer certaines obligations au personnel de l'hôpital.

87. L'APD ne considère pas de tels documents comme constituant une politique de sécurité de l'information permettant de démontrer que les mesures techniques et organisationnelles déterminées par le responsable de traitement garantissent un niveau de sécurité adapté au risque, en conformité avec le RGPD. Seule une politique de sécurité de l'information formelle et actualisée peut permettre au responsable de traitement de démontrer son niveau de conformité aux exigences du RGPD en matière de sécurité, sous réserve que son contenu soit complet, effectivement adapté au risque et correctement implémenté.

88. **En conclusion, la défenderesse n'est pas en mesure de démontrer sa conformité aux articles 5.1.f) et 32 du RGPD, par le biais d'une politique de sécurité de l'information formelle et actualisée au moment de la violation de données.**

II.3.3. Constatation 3 : Sur la politique et/ou la procédure de mise à jour de sécurité des équipements informatiques (logiciels)

89. **La défenderesse** soutient que la politique de mise à jour de sécurité des équipements informatiques est constituée des contrats de consultance conclus par l'hôpital afin d'assurer un contrôle mensuel de ses installations. Par ailleurs, elle mentionne

plusieurs mesures ayant été mises en place par l'hôpital postérieurement à la violation de données, notamment la mise en place d'un Web Application Firewall en mars 2022.

90. **La Chambre contentieuse** souligne que la défenderesse n'explique ni dans ses réponses au Service d'inspection, ni dans ses conclusions quelle était la politique et/ou la procédure de mise à jour de sécurité des équipements informatiques (logiciels) mise en place au moment de la violation de données.

91. Le rapport d'enquête a révélé que la faille de sécurité exploitée par le pirate informatique était due à une vulnérabilité sur le serveur Microsoft Exchange. L'exploitation de cette faille a permis au pirate informatique de mettre en place son attaque et de chiffrer un ensemble de serveurs accessibles. Le fait que seuls les firewalls et passerelles anti-virus étaient contrôlés n'était pas de nature à empêcher l'exploitation de ce type de failles de sécurité.

92. De fait, il ressort de l'enquête du Service d'inspection que la vulnérabilité exploitée par le pirate informatique était considérée comme « critique » de par sa facilité d'exploitation. Au vu des réponses fournies, la défenderesse ne démontre pas que ce type de risque était en mesure d'être détecté et géré au moment de la violation de données.

93. Outre les principes d'intégrité et de confidentialité, et les exigences de sécurité (articles 5.1.f) et 32 du RGPD), le RGPD impose au responsable de traitement de réexaminer et actualiser les mesures techniques et organisationnelles mises en place, si nécessaire (article 24 du RGPD). Le CEPD fait figurer la bonne gestion des correctifs (proper patch management) comme une des mesures de sécurité les plus importantes dans ses lignes directrices 01/2021 du 14 décembre 2021 concernant les exemples de notification des violations de données (cf. paragraphe 18)[23]. Les Normes minimales rappellent en outre que : « Toute organisation doit installer un système et des procédures formelles et actualisées permettant la détection, le suivi et la réparation d'infractions au niveau de la sécurité proportionnellement au risque technique / opérationnel ».

94. Il ressort du rapport du Service d'inspection que le responsable de traitement n'avait pas mis en place des mesures capables de l'alerter sur le fait que son traitement de

[23] CEPD, Lignes directrices 01/2021, Exemples concernant la notification de violations de données à caractère personnel, adoptées le 14 décembre 2021, v2.0, disponibles sur le lien suivant : https://www.edpb.europa.eu/system/files/2022-09/edpb_guidelines_012021_pdbnotification_adopted_fr.pdf

Voir également en ce sens, la version précédente de ces lignes directrices (pour consultation publique), du 14 janvier 2021, qui mentionne déjà ces recommandations au paragraphe 18 : https://www.edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_202101_databreachnotificationexamples_v1_en.pdf

données personnelles ne garantissait pas une sécurité appropriée aux risques. Malgré les prescriptions de l'article 24 du RGPD, et l'obligation faite au responsable du traitement d'être en mesure de démontrer le respect des principes de base du RGPD en vertu de l'article 5.2 du RGPD, la défenderesse ne démontre ni quelles mesures techniques et organisationnelles étaient mises en place au moment de la violation de données s'agissant de la sécurité des logiciels, ni comment celles-ci faisaient l'objet d'une quelconque réexamination ou actualisation.

95. Quand bien même la défenderesse énumère un grand nombre de mesures ayant été mises en place, celles-ci ne l'ont été que postérieurement à la violation.

96. **En conclusion, la Chambre contentieuse considère que la défenderesse a manqué à son obligation de prévoir une politique et/ou une procédure de mise à jour de sécurité des équipements informatiques (logiciels) au moment de la violation de données, et donc enfreint les articles 5.1.f), 32 et 24 du RGPD du fait de l'insuffisance de ces mesures techniques et leur actualisation.**

II.3.4. Constatation 4 : Sur les autres mesures de sécurité

Sur le programme de formation/sensibilisation des employés

97. **La défenderesse** soutient que l'hôpital dispose d'un « véritable programme de sensibilisation des employés », composé notamment d'une formation sur le hameçonnage effectuée suite à la première violation de données de 2019, de la charte informatique remise aux employés à leur embauche, de leurs obligations de confidentialité, d'exercices de sécurité, de la formation sur le PUH et de la participation par certains employés aux journées Cyber-Europe.

98. **La Chambre contentieuse** rappelle que l'article 32 du RGPD impose au responsable de traitement de mettre en œuvre des mesures techniques et organisationnelles appropriées pour garantir un niveau de sécurité adapté au risque. L'article 5 impose de traiter les données personnelles de façon à garantir une sécurité appropriée des données à caractère personnel. De plus, l'article 24 du RGPD précise que le responsable de traitement doit réexaminer et actualiser ces mesures, si nécessaire.

99. Les employés d'un hôpital en contact avec des catégories spéciales de données personnelles doivent recevoir une formation appropriée et régulière relative aux normes de sécurité minimales à respecter dans le cadre du traitement de telles données, en fonction de la pertinence pour leur rôle ou fonction.

100. Cette formation continue fait partie intégrante des mesures organisationnelles qui doivent être mises en place par l'hôpital afin d'assurer la sécurité des données. Elle doit être régulièrement actualisée pour prévenir les risques de violation de données.

En effet, dans un contexte où les hôpitaux sont sujets à des menaces croissantes de cyberattaques, il est essentiel de maintenir une formation à jour afin de garantir la conformité aux exigences réglementaires et de protéger efficacement les données personnelles.

101. Contrairement à ce que soutient la défenderesse, la Chambre contentieuse ne peut considérer qu'un véritable programme de formation / sensibilisation des employés soit mis en place par l'hôpital. Aucun des documents cités au paragraphe 97, même pris ensemble, ne constitue un véritable programme de formation continue et systématique au RGPD tel que requis par l'article 32 du RGPD. Une formation sur le hameçonnage, bien qu'utile, ne suffit pas à couvrir les aspects importants de la protection des données personnelles.

102. De plus, la charte informatique remise à l'embauche et les obligations de confidentialité, sans suivi régulier et mise à jour pertinentes, ne permettent pas de considérer que les employés soient régulièrement informés des bonnes pratiques en matière de protection de la confidentialité des données, d'autant plus que les risques évoluent constamment.

103. Les exercices de sécurité et la formation sur le PUH n'ont pas pour objet d'assurer une formation quant aux principes de protection et de sécurité des données personnelles. Enfin, la participation ponctuelle de certains employés aux journées Cyber-Europe ne remplace pas une formation structurée et continue pour l'ensemble du personnel. L'hôpital ne démontre aucune démarche proactive et régulière quant à la formation / sensibilisation de son personnel aux exigences spécifiques du RGPD.

104. Pendant l'audition, la défense a expliqué que des membres du personnel ont la possibilité de suivre des formations en matière de cybersécurité. Des membres du personnel hospitalier ont assisté à la cyberweek en octobre 2023, dont le thème traite de la cybersécurité dans le secteur de la santé. Elle justifie également l'intervention d'un prestataire extérieur, qui a permis de former une vingtaine de « champions RGPD ». La Chambre contentieuse prend note de ces efforts et confirme qu'ils vont dans le bon sens, mais force est de constater que ces formations ne s'appliquent qu'à une infime proportion des membres du personnel et ont été mises en place postérieurement à la violation de données.

105. **En conclusion, l'hôpital ne disposait pas d'un véritable programme de formation / sensibilisation des employés au RGPD et a de ce fait violé les articles 32, 5.1.f) et 24 du RGPD.**

Sur le système de préservation des logs en vue d'analyse ultérieures lors d'incidents

106. **La défenderesse** affirme que l'hôpital dispose d'un système de préservation des logs, lequel était mis en place avant la violation de données. Cependant, elle admet que l'attaquant a sciemment supprimé une partie de ces logs afin de tenter d'effacer les traces de son passage. Pendant l'audition, la défenderesse a cependant affirmé que les logs n'ont pas été supprimés (contrairement à la défense présentée dans ses conclusions), mais « chiffrés » par l'attaquant.

107. **La Chambre contentieuse** rappelle l'obligation imposée au responsable de traitement de mettre en œuvre des mesures techniques et organisationnelles appropriées pour garantir un niveau de sécurité adapté au risque, notamment la capacité à assurer la confidentialité, l'intégrité, la disponibilité et la résilience constante des systèmes et services de traitement (32.1.b) du RGPD). Cela inclut également la capacité à préserver des logs en vue d'analyses ultérieures lors de violations de données.

108. La Chambre contentieuse constate que la défenderesse semble confondre les concepts de journalisation des logs et de préservation des logs. La préservation des logs, dont il est question, a précisément pour but d'empêcher la suppression ou le chiffrage des logs. Cette préservation est cruciale pour analyser a posteriori les actions effectuées sur les données personnelles. En principe, un tel système de préservation des logs devrait permettre de déterminer pendant une durée raisonnable qui a eu accès à quelles informations, à quel moment et de quelle manière, ainsi que l'identification de la nature des informations consultées et l'identification précise de la personne. Ces logs devraient être stockés de manière ségréguée sur des équipements distincts, protégés contre le chiffrement, garantissant ainsi une traçabilité fiable et sécurisée. La Chambre contentieuse rappelle que les Normes minimales précitées contiennent des exigences précises et spécifiques en matière de préservation des logs, qui constituent une bonne pratique à suivre lors de l'implémentation d'un tel système.

109. En l'espèce, la défense confirme dans ses conclusions, que l'attaquant a sciemment supprimé une partie de ces logs afin de tenter d'effacer les traces de son passage, à l'exception d'un serveur (radiologie) où il a laissé des indices. Cette absence de préservation des logs rend difficile la compréhension de l'attaque, l'identification des failles exploitées et l'évaluation des données compromises. La défenderesse explique que, lors de la violation de données, les logs du firewall n'ont pas été effacés, et que leur analyse a permis de confirmer que « ce sont probablement des actions et des commandes qui ont été exportées par les attaquants, et non des données à caractère personnel ». Or, en l'absence de préservation de logs, il est impossible à la défenderesse de démontrer de telles hypothèses.

110. Pendant l'audition, la défenderesse soutient, en contradiction avec ces conclusions, que les logs n'ont pas été « effacés », mais « chiffrés ». Quand bien même les logs auraient été chiffrés, plutôt qu'effacés, la défenderesse démontre que les logs n'ont pas pu être préservés en vue de leur analyse ultérieure.

111. Cette situation met en lumière une absence, ou à tout le moins, une insuffisance dans le système de préservation des logs de l'hôpital au moment de la violation de données (voir en ce sens les paragraphes 19, 28 et 49 des lignes directrices 01/2021 du CEPD, concernant les exemples de notification des violations de données personnelles).

112. Pendant l'audition, la défenderesse a expliqué que toutes les améliorations apportées aux back-ups prises par l'hôpital empêchent désormais de supprimer les logs, et que s'ils sont supprimés, ils peuvent désormais être récupérés. La Chambre contentieuse prend note de la mise en place de cette mesure technique, même si son implémentation intervient tardivement, en particulier si l'on prend en considération qu'une première violation de données avait déjà eu lieu en 2019.

113. **Par conséquent, au moment de la violation de données, l'hôpital a violé les exigences de sécurité des articles 5.1.f), 24 et 32 du RGPD en ne mettant pas en place des mesures adéquates pour préserver les logs contre des suppressions malveillantes ou le chiffrement, compromettant ainsi la capacité à détecter et analyser des violations de données, en vue de leur documentation ultérieure.**

Sur les audits systématiques de la qualité de la sécurité des données personnelles

114. **La défenderesse** explique qu'elle a pris des mesures contractuelles pour s'assurer que différents prestataires interviennent afin d'auditer les systèmes de l'hôpital, la sécurité et la qualité des données. Ces mesures ont été prises postérieurement à la seconde violation de données.

115. **La Chambre contentieuse** rappelle que l'article 32.1.d) du RGPD propose une série de mesures techniques et organisationnelles, notamment, selon les besoins, une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement.

116. Un audit de la qualité de la sécurité des données permet d'analyser les infrastructures informatiques et d'identifier les points faibles des systèmes de gestions des informations (y compris des données personnelles), notamment du matériel, des logiciels, des données et des procédures, en vue de garantir un niveau de sécurité adéquat au risque. Un rapport d'audit détaillé permet au responsable de traitement de connaître les zones vulnérables exposées aux cybercriminels. Sur la base d'un tel

rapport, une cartographie des risques est établie et des mesures de sécurité adéquates sont préconisées pour réduire les risques identifiés.

117. Les Normes minimales rappellent que toute organisation doit « réaliser périodiquement un audit de conformité de la situation relative à la sécurité de l'information et à la vie privée telle que décrite dans les politiques », et ce au moins une fois par an. L'enquête menée par le Service d'inspection a démontré qu'aucun audit de la qualité de la sécurité des données personnelles n'avait été effectué au moment de la violation. Les documents fournis par la défenderesse montrent que plusieurs audits ont été réalisés après la violation de données.

118. Cependant, ces audits postérieurs ne suffisent pas à démontrer que l'hôpital a fait preuve des diligences nécessaires pour prévenir les violations de données à travers des audits systématiques avant la seconde violation de données. Cette absence d'audits a pu contribuer à la survenance de la seconde violation de données, révélant une insuffisance dans la gestion proactive de la sécurité des données personnelles. En outre, la Chambre contentieuse invite l'hôpital à s'assurer que les audits mis en place postérieurement à la seconde violation de données répondent aux exigences explicitées dans le paragraphe 116.

119. **En conclusion, la défenderesse a manqué à son obligation de sécurité en n'ayant pas mis en place des audits réguliers et systématiques pour tester, analyser et évaluer l'efficacité des mesures techniques et organisationnelles au moment de la violation, et assurer la sécurité des traitements de données comme l'exigent les articles 32, 24 et 5.1.f) du RGPD.**

Sur la sécurisation du mot de passe d'accès au dossier informatisé du patient

120. **La défenderesse** estime qu'elle dispose d'une forte sécurisation des mots de passe d'accès aux dossiers informatisés des patients. Elle l'explique par le fait que pour accéder aux dossiers des patients informatisés, chaque utilisateur doit avoir accès au logiciel dédié de l'hôpital installé en local sur les ordinateurs et autres appareils de l'hôpital, et remplir un formulaire de demande d'accès. Ce formulaire nécessite un identifiant et la création par l'utilisateur d'un mot de passe. À l'époque de l'attaque, ce mot de passe devait contenir entre 6 et 8 caractères, et ne pas correspondre au prénom, au nom, au service ou aux initiales de l'utilisateur. L'hôpital explique être tributaire du fournisseur de son logiciel de gestion des dossiers médicaux pour définir les critères de mots de passe.

121. **La Chambre contentieuse** rappelle que le RGPD impose au responsable de traitement de mettre en œuvre des mesures techniques et organisationnelles appropriées pour garantir un niveau de sécurité adapté au risque. Ces mesures

incluent, entre autres, la capacité à garantir la confidentialité permanente des systèmes et services de traitement (article 32.1.b) du RGPD).

122. Dans un contexte hospitalier, où la protection des données de santé des patients est cruciale, un mot de passe très robuste est nécessaire. Des recommandations sur la sécurisation des mots de passe peuvent être trouvées dans les normes telles que celles de l'Agence européenne pour la cybersécurité (ENISA) et les directives de l'Institut national des normes et de la technologie (NIST). De plus, la Note de sécurité de l'information & protection de la vie privée : Synthèse et règles pratiques en matière de protection de données médicales, du 14 juillet 2017 élaborée sur la base des discussions au sein du sous-groupe de travail « données médicales » du Comité de sécurité de l'information[24], prévoit que « Un mot de passe suffisamment long compte minimum 12 caractères ». Or, un mot de passe de 6 à 8 caractères est faible. Il ne peut permettre de faire face aux attaques par force brute et ne constitue pas un moyen d'authentification forte.

123. La défense soutient dans ses conclusions que la politique de mot de passe a été renforcée au sein de l'hôpital, et qu'il doit désormais faire au moins 8 caractères. Toutefois, sur la base des démonstrations dans le paragraphe précédent, la Chambre contentieuse considère la longueur d'un tel mot de passe comme insuffisante sur la base des critères énoncés à l'article 32.1 du RGPD, en particulier compte tenu de l'état des connaissances, du contexte et des risques auxquels fait face l'hôpital.

124. Par ailleurs, si la défenderesse avance que chaque utilisateur doit avoir accès au logiciel dédié de l'hôpital et remplir un formulaire de demande d'accès pour justifier le caractère adéquat de la sécurisation de son mot de passe, la Chambre contentieuse invite la défenderesse à considérer la mise en place d'un mécanisme de double authentification, envisagé comme une mesure technique appropriée aux risques. Comme rappelé dans les lignes directrices sur la notification de violations de données du WP29[25] : « Si des données médicales critiques concernant les patients d'un hôpital sont rendues indisponibles, ne serait-ce que temporairement, cela pourrait présenter un risque pour les droits et libertés des personnes concernées; des opérations pourraient par exemple être annulées et des vies mises en danger ».

125. Par ailleurs, le fait que l'hôpital était tributaire de critères de mots de passe insuffisants définis par son fournisseur, signifie que l'hôpital a fait appel à un sous-

[24] Voir la catégorie « Documents complémentaires », et « NOTA MEDSEC Synthèse et règles Protection données médicales », accessible ci-contre : https://www.ksz-bcss.fgov.be/fr/protection-des-donnees/politique-de-securite-de-l-information

[25] Ces Lignes directrices sur la notification de violations de données à caractère personnel en vertu du règlement (UE) 2016/679 ont été publiées par le WP29 (prédécesseur du CEPD). Elles sont accessibles depuis le lien suivant : https://ec.europa.eu/newsroom/article29/items/612052/en (voir page 9)

traitant qui présentait des garanties insuffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées.

126. **En conclusion, la défenderesse n'a pas tenu compte des critères des articles 32, 5.1.f) et 24 du RGPD pour ajuster la robustesse du mot de passe au niveau de sécurité requis pour protéger l'accès à des dossiers informatisés de patients.**

III. Sanctions

III.1. Sur la qualification juridique de la défenderesse

127. La Chambre contentieuse a tenu compte des réponses apportées par la défenderesse au formulaire de sanction et des statuts de l'hôpital[26] dans son analyse.

128. L'article 221§2[27] de la Loi cadre contient une exception, concernant l'imposition d'une amende aux « autorités publiques », sous certaines conditions. La notion « d'autorité publique » est définie à l'article 5[28] de la Loi cadre. Les critères pertinents de l'article 5.3° de la Loi cadre qui ont été soulevés par la défenderesse pour démontrer que la défenderesse devrait être qualifiée « d'autorité publique » seront analysés successivement ci-dessous.

129. A titre liminaire, il n'est pas contesté que l'hôpital est doté de la personnalité juridique en tant qu'Association Sans But Lucratif (ci-après « ASBL »), conformément à la deuxième condition de l'article 5.3° de la Loi cadre.

Satisfaction spécifique de besoin d'intérêt général

---

[26] [...]

[27] L'article 221§2 de la Loi cadre prévoit que : « L'article 83 du Règlement ne s'applique pas aux autorités publiques et leurs préposés ou mandataires sauf s'il s'agit de personnes morales de droit public qui offrent des biens ou des services sur un marché ».

[28] L'article 221§2 de la Loi cadre prévoit que : « L'article 83 du Règlement ne s'applique pas aux autorités publiques et leurs préposés ou mandataires sauf s'il s'agit de personnes morales de droit public qui offrent des biens ou des services sur un marché ».

[28] L'article 5 de la Loi cadre, prévoit que : « Pour l'application de la présente loi, on entend par "autorité publique" :

1° l'état fédéral, les entités fédérées et les autorités locales;

2° les personnes morales de droit public qui dépendent de l'Etat fédéral, des entités fédérées ou des autorités locales;

3° les personnes, quelles que soient leur forme et leur nature qui :

- ont été créées pour satisfaire spécifiquement des besoins d'intérêt général ayant un caractère autre qu'industriel ou commercial; et

- sont dotées de la personnalité juridique; et

- dont soit l'activité est financée majoritairement par les autorités publiques ou organismes mentionnés au 1° ou 2°, soit la gestion est soumise à un contrôle de ces autorités ou organismes, soit plus de la moitié des membres de l'organe d'administration, de direction ou de surveillance sont désignés par ces autorités ou organismes;

4° les associations formées par une ou plusieurs autorités publiques visées au 1°, 2° ou 3° ».

130. La défenderesse s'appuie principalement sur l'objet social de l'hôpital défini dans ses statuts comme visant à « améliorer le sort matériel et moral des habitants de (...) », pour démontrer que l'hôpital satisfait des besoins d'intérêt général, conformément à la première condition de l'article 5.3° de la Loi cadre.

131. Or, selon la Chambre contentieuse, cette formulation telle qu'elle ressort de l'objet social ne suffit pas à établir que l'hôpital a été créé « spécifiquement » pour des besoins d'intérêt général, tel que requis par l'article 5.3° de la Loi cadre.

132. En effet, les tribunaux ont reconnu que les hôpitaux poursuivent d'une manière durable un but économique, fut-ce habituellement à l'appui de leurs objectifs en principe altruistes[29]. Il est donc clair que leur activité, bien que couverte par un cadre altruiste, s'inscrit dans une démarche où la viabilité financière et la recherche d'efficacité économique sont des composantes importantes, même si l'hôpital est constitué sous la forme d'une ASBL. Par conséquent, la création de ces entités n'est pas exclusivement orientée vers la satisfaction de besoins d'intérêt général, mais intègre également des considérations économiques qui ne peuvent être ignorées dans l'appréciation de leur qualification juridique au sens de l'article 5.3 de la Loi cadre.

133. L'hôpital n'a pas été créé « spécifiquement » pour des besoins d'intérêt général, et obéit à une logique économique propre, de sorte que la première condition de l'article 5.3° de la Loi cadre n'est pas remplie.

Financement de l'hôpital :

134. Dans sa réponse au formulaire de sanction, la défenderesse a exposé de manière détaillée les revenus de l'hôpital sous la forme de cinq sources de revenus principales, dont la quasi-totalité serait, selon elle, un financement par les autorités publiques, de sorte que la dernière condition de l'article 5.3° de la Loi cadre serait remplie.

135. Trois des cinq sources de revenus proviennent d'autorités publiques. Toutefois, deux sources de financement méritent une analyse détaillée. Celles-ci représentent la majorité du financement de l'hôpital sur la base des chiffres rapportés par la défenderesse[30]. En effet, selon les chiffres fournis par la défenderesse, près de la moitié (..%) de ses revenus proviennent des « honoraires des médecins » et (..%) de la « vente de produits pharmaceutiques ».

---

[29] Voir sur ce point l'affaire Civ. Flandre orientale (div. Gand) (2e ch.) du 27 avril 2015, qui rappelle que les acteurs de ce que l'on appelle le « secteur social profit », comme les hôpitaux, relèvent le plus souvent de la notion d' « entreprise », dès lors qu'ils poursuivent d'une manière durable un but économique, fut-ce habituellement à l'appui de leurs objectifs en principe altruistes. Dans cette affaire, le fait que la demanderesse avait la forme d'une association sans but lucratif n'y faisait pas obstacle. Elle a été considérée comme une entreprise, même sans but lucratif.

[30] Les revenus de 2021 et 2023 ont été fournis par la défenderesse. La Chambre contentieuse s'est servie des chiffres rapportés en 2023, même si l'analyse aurait été très similaire avec les chiffres tirés de l'exercice de 2021.

136. Selon la défenderesse :

    a. Les honoraires des médecins, facturés essentiellement à l'INAMI[31] via les organismes assureurs (Mutuelles et CAAMI[32]), consistent en la facturation des prestations, et des actes thérapeutiques des prestataires de soins à la Sécurité sociale.

    b. Les recettes en lien avec la vente de produits pharmaceutiques résultent de la facturation des médicaments essentiellement à l'INAMI via les organismes assureurs (Mutuelles et CAAMI) et aux patients, le cas échéant sous la forme de forfaits.

137. Toujours selon la défenderesse : « Bien que les Mutuelles soient des personnes morales de droit privé, ces dernières sont financées majoritairement par l'INAMI, personne morale de droit public dépendant de l'Etat fédéral, via l'assurance obligatoire qui intervient majoritairement ». Ainsi, la défenderesse considère que la source de financement de l'hôpital est très majoritairement publique puisqu'elle provient de l'INAMI, de sorte que l'hôpital devrait être qualifié d'autorité publique.

138. La Chambre contentieuse ne suit pas ce raisonnement. Certes, l'INAMI est une institution publique, mais son rôle se limite à rembourser une partie des soins prodigués aux patients dans le cadre de l'assurance maladie obligatoire. Ce mécanisme n'implique pas un financement direct des hôpitaux, mais relève d'un système complexe dans lequel chaque citoyen est tenu de souscrire une assurance maladie pour obtenir le droit à une participation de l'Etat à ses frais, au titre de la sécurité sociale. Le système de tiers payant permet aux patients de bénéficier de soins sans avoir à avancer la totalité des frais, mais cela n'implique pas que l'hôpital soit lui-même financé directement par l'INAMI.

139. Ce système unique de remboursement est fondamentalement distinct du concept de financement visé par l'article 5.3° de la Loi cadre. Ainsi, l'hôpital n'est pas financé majoritairement par les autorités publiques ou organismes mentionnés au 1° ou 2° de l'article 5 de la Loi cadre. La dernière condition de l'article 5.3° de la Loi cadre concernant le financement majoritaire par des autorités publiques n'est pas remplie.

La gestion est soumise à un contrôle des autorités publiques :

---

[31] L'INAMI est l'Institut national d'assurance maladie-invalidité. Il s'agit d'une institution fédérale.

[32] Dans l'hypothèse où un assuré n'est pas affilié à une mutuelle, la Caisse d'Assurance Auxiliaire de Maladie-Invalidité (CAAMI), institution publique de sécurité sociale, intervient dans le cadre de l'assurance obligatoire. Elle représente 100 000 membres ou 1% du marché. Cette source de financement est publique, ce qui n'est pas contesté par la Chambre contentieuse.

140. Selon la défenderesse, le système hospitalier belge est organisé par les pouvoirs publics. Elle soutient que l'Agence Wallonne pour une Qualité de Vie (« AVIQ ») est le service public régional wallon en charge de la gestion de l'agrément octroyé aux hôpitaux régionaux et de leur inspection. Par conséquent, la gestion de l'hôpital est soumise à un contrôle des autorités publiques selon la défenderesse. Par ailleurs, elle considère que les pouvoirs publics contrôlent tant à l'entrée (tarifs pratiqués par les hôpitaux) qu'à la sortie (dépenses effectuées).

141. La Chambre contentieuse rejette une nouvelle fois les arguments avancés par la défenderesse, en distinguant clairement les concepts de réglementation et de contrôle effectif de la gestion. Certes, l'Agence Wallonne pour une Qualité de Vie (« AVIQ ») assure une mission d'inspection et d'octroi d'agréments, mais ces fonctions relèvent uniquement de la supervision réglementaire visant à garantir le respect de normes spécifiques en matière de qualité des soins. Ces mécanismes de contrôle externe, bien que nécessaires pour garantir la sécurité et la qualité, ne sauraient être confondus avec un contrôle direct de la gestion interne des hôpitaux par les pouvoirs publics.

142. La gestion de l'hôpital, en tant qu'ASBL, est soumise au Code des sociétés et des associations, qui régit ses activités internes comme celles de toute entité privée. Les organes décisionnels de l'hôpital, à savoir le conseil d'administration et l'assemblée générale, sont exclusivement composés de personnes privées, comme le stipulent les articles 6, 7 et 11 des statuts de l'association. Aucune disposition statutaire ou légale n'impose la présence de représentants des autorités publiques au sein de ces organes. En outre, les décisions relatives à la stratégie financière, au recrutement du personnel, ou encore à la gestion des infrastructures, sont prises sans ingérence des pouvoirs publics.

143. Le cadre législatif impose certaines obligations aux hôpitaux en termes de tarifs et de dépenses, mais il ne s'agit pas d'un contrôle financier direct. Les autorités publiques ne décident pas de l'affectation des ressources ou de la gestion des budgets hospitaliers. Ces derniers relèvent des organes de gestion internes de l'hôpital, qui conservent une autonomie de décision et une responsabilité propre en matière de gestion financière. En outre, l'Assemblée générale de l'hôpital peut décider, sans ingérence des autorités publiques, de dissoudre l'hôpital (article 39 des statuts).

144. Enfin, les débats parlementaires concernant la Loi cadre démontrent que le législateur n'a jamais envisagé l'idée que les hôpitaux ayant la forme d'ASBL soient écartés du régime des amendes administratives prévu par le RGPD et la Loi cadre. Même dans des cas d'espèce plus complexes que la présente affaire, où un hôpital est géré par un Centre Public d'Action Sociale (« CPAS »), les parlementaires soutenaient qu'un tel

hôpital soit soumis au régime des amendes administratives : « Des organisations qui, sur le fond, exercent les mêmes activités, doivent être traitées de la même manière, qu'elles appartiennent au secteur public ou privé. Ainsi, il est par exemple injustifiable qu'un hôpital géré par un CPAS ne puisse se voir infliger une amende administrative, alors que cela pourrait être le cas pour un hôpital ayant la forme juridique d'une ASBL »[33] (soulignement ajouté).

145. Ainsi, l'hôpital, bien que soumis à une réglementation et à des inspections, reste une entité autonome dont la gestion ne peut être assimilée à un contrôle des autorités publiques tel que défini par l'article 5 de la Loi cadre. La dernière condition de l'article 5.3° de la Loi cadre concernant la gestion par les autorités publiques n'est pas remplie. En conclusion, la Chambre contentieuse retiendra la qualification de la Y comme ASBL de droit privé, sans lien de lien de préposition ou de mandat entre l'hôpital et une quelconque autorité publique. Cette qualification lui empêche de prétendre à l'exception prévue par l'article 221§2 de la Loi cadre, s'agissant de l'imposition d'une amende sur la base de l'article 83 du RGPD.

146. Afin de lever toute ambiguïté, la défenderesse est d'accord pour considérer que l'article 221§2 de la Loi cadre, qui prévoit que les personnes morales de droit public qui offrent des biens et/ou des services sur un marché ne sont pas exemptées de l'amende administrative, ne doit pas être examinée dans le cadre de la présente procédure. En effet, elle ne conteste pas que l'hôpital est une personne morale de droit privé.

III.2. Sur l'amende

147. La Chambre contentieuse a tenu compte des réponses apportées par la défenderesse au formulaire de sanction dans son analyse.

III.2.1. Rappel des dispositions légales applicables

148. En tant qu'autorité administrative indépendante, la Chambre contentieuse a le pouvoir exclusif de déterminer les mesures correctrices et les sanctions appropriées conformément aux dispositions pertinentes du RGPD et de la LCA. Cette compétence découle spécifiquement des articles 58 et 83 du RGPD, comme l'a confirmé la jurisprudence de la Cour des marchés dans ses arrêts du 7 juillet 2021, 19 février 2020

[33] Rapport présenté au nom de la Commission Justice par M. P. Dedecker, Documents parlementaires Chambre 2017-2018, n° 54-3126/3, p. 44, accessible depuis le lien suivant : https://www.dekamer.be/FLWB/PDF/54/3126/54K3126003.pdf

ou encore du 20 décembre 2023[34], qui ont mis en lumière l'étendue du pouvoir discrétionnaire de la Chambre contentieuse concernant le choix des sanctions et l'ampleur de l'amende.

149. Selon les lignes directrices du CEPD et le RGPD, l'autorité de contrôle a le pouvoir discrétionnaire d'imposer une amende[35]. Le RGPD exige de chaque autorité de contrôle qu'elle veille à ce que les amendes administratives imposées soient effectives, proportionnées et dissuasives dans chaque cas d'espèce (article 83.1 du RGPD).

150. De plus, lors de la détermination du montant de l'amende, l'autorité de contrôle doit tenir dûment compte, pour chaque cas d'espèce, de plusieurs éléments spécifiques, tels que « *la nature, la gravité et la durée de la violation, compte tenu de la nature, de la portée ou de la finalité du traitement concerné, ainsi que du nombre de personnes concernées affectées et le niveau de dommage qu'elles ont subi* » (article 83.2. a) du RGPD) ; ainsi que « *la nature intentionnelle ou négligente de la violation* » (article 83.2. b) du RGPD) ; et « l*es catégories de données à caractère personnel concernées par la violation* » (article 83.2. g) du RGPD).

151. En conséquence, toute amende[36] doit être évaluée en tenant compte de l'ensemble des facteurs énoncés à l'article 83.2, points a) à k) du RGPD, sans pour autant excéder le montant maximal légal fixé à l'article 83.4 à 83.6 du RGPD.

152. Conformément au considérant 148 du RGPD, des sanctions, y compris des amendes administratives, doivent être imposées en complément ou à la place des mesures appropriées en cas de manquement grave, même lorsqu'il s'agit de la première constatation d'un manquement[37]. Ainsi, le fait qu'un comportement infractionnel ne soit constaté que pour la première fois dans le chef d'une défenderesse n'empêche pas la Chambre contentieuse de pouvoir imposer une amende administrative, conformément à l'article 58.2. i) du RGPD.

---

[34] Cour des marchés, 19ème Chambre A, arrêt du 7 juillet 2021, 2021/AR/320 (accessible ici), p. 37-47 ; Cour des marchés, 19ème Chambre A, arrêt du 19 février 2020, 2020/AR/1160, (accessible ici) p. 30-31 ; Cour des marchés, 19ème Chambre A, arrêt du 20 décembre 2023, 2023/AR/817, (accessible ici) p. 57, 61 et 62.

[35] CEPD - Lignes directrices 04/2022 sur le calcul des amendes administratives au titre du RGPD, adoptées le 24 mai 2023 (v2.1), disponible sur le site : https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-042022-calculation-administrative-fines-under_fr, voir points 15, 20, 69, 84, 144. ; RGPD, considérants 148, 150 ; art. 58.1.i), 83.

[36] CJUE, Arrêt du 5 décembre 2023, Deutsche Wohnen SE contre Staatsanwaltschaft Berlin, C-807/21, EU:C:2023:950 ; CJUE, Arrêt du 5 décembre 2023, Nacionalinis visuomenės sveikatos centras, C-683/21, ECLI:EU:C:2023:949,

[37] CJUE, 5 décembre 2023, C-807/21, *Deutsche Wohnen SE c. Staatsanwaltschaft Berlin* (ECLI:EU:C:2023:950), point 38.

III.2.2. Raisons de l'imposition d'une amende

153. La CJUE a jugé récemment qu'en cas de constatation d'une violation de données à caractère personnel, l'autorité de contrôle n'est pas tenue d'adopter une mesure correctrice, en particulier une amende administrative, au titre de l'article 58.2 du RGPD, lorsqu'une telle intervention n'est pas appropriée, nécessaire ou proportionnée pour remédier à l'insuffisance constatée et garantir le plein respect de ce règlement[38].

154. La Chambre contentieuse décide d'imposer une amende administrative car elle considère que, dans les circonstances spécifiques de l'affaire exposées ci-dessous, en tenant compte des critères pertinents repris à l'article 83.2 du RGPD, une amende est appropriée. Les critères pertinents précités ne valent donc pas uniquement lors de l'imposition d'une amende conformément à l'article 83, paragraphe 1 du RGPD mais également lors du choix entre les différents types de sanctions qui sont prévues à l'article 58, paragraphe 2 du RGPD et à l'article 100 de la LCA[39].

155. Pour décider qu'une amende administrative était appropriée en l'espèce, la Chambre contentieuse retient les critères suivants[40] :

- **La gravité des violations :** En tenant compte de la nature sensible des données traitées dans ce contexte hospitalier, les violations retenues revêtent une gravité particulière. Les données de santé, de par leur caractère sensible, bénéficient d'un régime de protection renforcé et méritent une protection « plus élevée »[41]. Les hôpitaux sont particulièrement vulnérables aux violations de données. Si certaines de ces violations sont inévitables en dépit de la mise en place de mesures techniques et organisationnelles appropriées, d'autres peuvent être prévenues. Pour les prévenir, le RGPD prévoit d'adapter ces mesures de sécurité au risque présenté par le traitement, ainsi que de mettre en place une AIPD pour mieux gérer les risques en amont et déterminer les mesures adéquates. Il apparaît clairement que les mesures techniques et organisationnelles en place lors de la violation de données survenue en 2021 n'étaient ni suffisantes ni conformes aux obligations légales, notamment celles imposées par l'article 32 du RGPD. Ce manquement est d'autant plus grave qu'il survient après une précédente violation de données de même nature (ransomware). Cette circonstance aurait dû inciter l'hôpital à ré-évaluer ses risques et

[38] Arrêt de la CJUE, C-768/21, du 26 Septembre 2024, ECLI:EU:C:2024:785

[39] S'agissant des conditions permettant d'apprécier l'opportunité d'imposer une amende, la Chambre contentieuse rappelle que ces conditions sont établies en détail dans les Lignes directrices sur l'application et la fixation des amendes administratives aux fins du règlement (UE) 2016/679, adoptées le 3 octobre 2019 par le Groupe de Travail WP29, accessibles sur le lien suivant : https://ec.europa.eu/newsroom/article29/items/611237/en

[40] Cour des marchés, 19ème Chambre A, arrêt du 19 février 2020, 2020/AR/1160, p. 30-31 ; Ces critères peuvent également être utilisés pour évaluer le montant de l'amende, conformément aux Lignes directrices du 3 octobre 2019 précitées.

[41] Voir l'article 9 et le considérant 55 du RGPD

renforcer ses mesures de sécurité adéquatement, y compris par la réalisation d'une AIPD. Le fait qu'un établissement hospitalier, responsable du traitement des données personnelles de 300 000 patients, n'ait pas pris toutes les mesures nécessaires pour prévenir une seconde violation de données, constitue une faute justifiant la sanction la plus dissuasive.

- **La durée de la violation** : Les mesures techniques et organisationnelles adéquates pour prévenir une nouvelle violation de données similaire auraient dû être mises en place au plus tard après la première violation de données. Or, la Chambre contentieuse relève que beaucoup de mesures de sécurité ont été mises en place seulement après la seconde violation de données, à savoir 2 ans et 6 mois après cet événement, et que cette mise en place était incomplète. Compte tenu des risques auxquels sont confrontés les hôpitaux, et du niveau de protection plus élevé attaché aux données de santé, les hôpitaux ne peuvent pas bénéficier d'une flexibilité importante dans les délais d'implémentation de leurs mesures de sécurité et de prévention des risques. L'hôpital n'a pas pris la mesure de l'urgence de mettre toutes ses mesures de sécurité en conformité, et ce, même après sa première violation de donnée en 2019. Cette durée justifie une réponse adaptée de la Chambre contentieuse.

- **L'effet dissuasif nécessaire pour prévenir de futures violations** : La Chambre contentieuse considère qu'il est regrettable que l'hôpital n'ait pas pris les mesures techniques et organisationnelles appropriées en amont, afin de mettre tout en œuvre pour éviter sa seconde violation de données. Un simple avertissement manquerait de produire l'effet dissuasif qu'il incombe aux autorités de contrôle de prendre en considération dans la détermination de la sanction appropriée. Une mesure d'ordre de mise en conformité, prise seule, pourrait amener l'hôpital et l'ensemble des hôpitaux belges à considérer que la constatation de tels manquements par la Chambre contentieuse constitue le point de départ de leur exercice de mise en conformité, ce qui compromettrait gravement les exigences de sécurité du RGPD. En faisant le choix d'imposer une amende, la Chambre contentieuse souligne la gravité de ces violations et la nécessité d'une diligence accrue dans la sécurisation des données personnelles en milieu hospitalier. Elle souhaite en particulier démontrer que des violations de données résultant d'une négligence sérieuse et persistante dans la gestion des risques peuvent entraîner des sanctions sévères.

156. Compte tenu du contexte qui ressort d'une telle évaluation, la Chambre contentieuse a déterminé qu'une amende administrative constitue la sanction adéquate pour envoyer un message fort, non seulement à la défenderesse, mais également à l'ensemble des hôpitaux belges. Cette sanction est la preuve que la non-conformité aux exigences du RGPD entraîne des sanctions sévères lorsque la gravité de la violation le justifie, comme en l'espèce.

III.2.3. Montant de départ du calcul de l'amende administrative

157. De manière à imposer une amende effective, proportionnée et dissuasive en tout état de cause, les autorités de contrôle sont censées ajuster les amendes administratives tout en restant dans la fourchette prévue dans les lignes directrices du CEPD[42] jusqu'au montant maximal légal. Cela peut conduire à des majorations ou des minorations significatives de l'amende, selon les circonstances du cas d'espèce.

i. Classification sur la base des violations au titre de l'article 83, paragraphes 4 et 5 du RGPD[43]

158. Le RGPD distingue deux catégories de violations : celles punissables selon l'article 83.4 du RGPD, d'une part, et celles punissables au titre de l'article 83.5 et 83.6 du RGPD, d'autre part. La première catégorie de violations entraîne une amende maximale de 10 millions d'EUR ou de 2 % du chiffre d'affaires annuel de l'entreprise, le montant le plus élevé étant retenu. Quant à la seconde catégorie, elle peut donner lieu à une amende maximale de 20 millions d'EUR ou de 4 % du chiffre d'affaires annuel de l'entreprise, le montant le plus élevé étant également retenu.

159. En l'espèce, la Chambre contentieuse constate la violation de plusieurs articles, à savoir les articles suivants :

- Article 35.3 du RGPD, relatif à l'analyse d'impact de protection des données
- Article 32 du RGPD, relatif à la sécurité du traitement
- Article 5.1.f) du RGPD, relatif au principe d'intégrité et de confidentialité
- Article 24 du RGPD, relatif à la responsabilité du responsable de traitement

160. L'amende la plus élevée s'applique, conformément à l'article 83.5.b) du RGPD. En effet, en cas de violation de l'article 5 (en l'espèce, le principe d'intégrité et de confidentialité), la Chambre contentieuse peut imposer une amende administrative allant jusqu'à 20.000.000 EUR ou, dans les cas d'une entreprise, jusqu'à 4% de son chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu.

161. **Dans le cas d'espèce, il apparaît que le chiffre d'affaires de la défenderesse est établi à (.. EUR) pour l'année 2023, laquelle précède l'année à laquelle sera rendue la décision dans la présente affaire et constitue donc l'exercice de référence. Sur**

---

[42] CEPD - Lignes directrices 04/2022 sur le calcul des amendes administratives au titre du RGPD, adoptées le 24 mai 2023 (v2.1), voir points 21 à 45.

[43] CEPD - Lignes directrices 04/2022 sur le calcul des amendes administratives au titre du RGPD, adoptées le 24 mai 2023 (v2.1), disponible sur le site https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-042022-calculation-administrative-fines-under_fr, voir points 49 et 50.

cette base, le plafond de l'amende la plus élevée encourue s'élève à 20.000.000 EUR.

ii. Gravité de la violation dans chaque cas d'espèce

162. Les critères tels que présentés ci-dessous suivent la méthodologie établie par les Lignes directrices sur le calcul des amendes du CEPD[44]. La Chambre contentieuse rappelle qu'elle n'est pas tenue d'examiner les critères qui sont sans objet[45].

Nature, gravité et durée de la violation (article 83, paragraphe 2, point a) du RGPD)

163. *Premièrement,* s'agissant de la nature des violations du cas d'espèce, celles-ci consistent en une série de manquements à divers articles du RGPD :

- **Article 35.3 du RGPD** : L'absence d'AIPD a privé l'hôpital de la possibilité de mieux cartographier ses systèmes informatiques et ainsi d'initier une réflexion concernant les mesures appropriées pour faire face aux risques, notamment de violation de données.
- **Article 32 du RGPD** : L'insuffisance de mesures techniques et organisationnelles appropriées augmente le risque de violations de données et réduit la capacité du responsable de traitement à les documenter, mettant en péril la protection des données personnelles contre les accès non autorisés.
- **Article 5.1.f) du RGPD** : Des mesures de sécurité inadéquates compromettent le principe d'intégrité et de confidentialité en rendant les données vulnérables aux accès non autorisés, aux modifications et à la divulgation. Cela nuit directement à l'application de l'article 5.1.f) du RGPD, dont l'objectif est d'assurer que les données personnelles soient traitées de manière sécurisée.
- **Article 24 du RGPD** : Une insuffisance dans les mesures de sécurité, y compris un manque de mise à jour régulière, reflète une défaillance du responsable du traitement à respecter les obligations de l'article 24 du RGPD, qui exige l'implémentation et la mise à jour continue de mesures appropriées pour garantir et démontrer la conformité au RGPD.

164. *Deuxièmement*, s'agissant de la gravité de la violation, la Chambre contentieuse retiendra les éléments suivants :

- **Nature du traitement** : Le contexte hospitalier implique la gestion de données sensibles de personnes vulnérables à grande échelle, traitement pour lequel une attention toute

[44] CEPD - Lignes directrices 04/2022 sur le calcul des amendes administratives au titre du RGPD adoptées le 24 mai 2023 (v2.1), disponible sur le site : https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-042022-calculation-administrative-fines-under_fr, voir point 17

[45] CEPD - Lignes directrices 04/2022 sur le calcul des amendes administratives au titre du RGPD adoptées le 24 mai 2023 (v2.1), disponible sur le site : https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-042022-calculation-administrative-fines-under_fr, voir point 6

particulière doit être apportée aux mesures de sécurité afin de limiter les risques pour les personnes. En effet, le CEPD rappelle dans ses lignes directrices que les cas de rançongiciels impliquent des risques élevés[46], en prenant pour exemple un hôpital ayant subi une attaque de type rançongiciel avec indisponibilité des données pendant 2 jours.

- **Finalité du traitement relevant des activités principales** : Les traitements ayant fait l'objet de l'enquête concernent la gestion des systèmes informatiques de la défenderesse, en particulier les messageries du personnel et les dossiers médicaux, essentiels pour la sécurité des données des patients et, de ce fait, la continuité des soins.
- **Nombre de personnes concernées** : L'hôpital compte 300 000 patients en base de données, ce qui constitue la base de référence de personnes concernées par la violation. En effet, du fait que les données des patients ont été temporairement indisponibles, y compris depuis le logiciel supportant les dossiers médicaux, les données de santé des 300 000 patients de l'hôpital font partie de la violation de données[47]. Par ailleurs, ces 300 000 personnes sont concernées par les manquements constatés par le Service d'inspection, notamment la sécurisation du mot de passe d'accès à leurs dossiers médicaux informatisés. De plus, les employés de l'hôpital ont eux aussi été impactés par la violation de données, du fait de l'inaccessibilité temporaire de leurs boîtes électroniques et des dossiers patients informatisés, à savoir leurs principaux outils de travail.
- **Niveau de dommage**[48] : La Chambre contentieuse retient que l'insuffisance des mesures techniques et organisationnelles de la défenderesse a contribué à rendre possible la violation de données de 2021. La continuité des soins des patients au niveau du service d'urgence a été perturbée pendant 3 jours et a causé la redirection des patients devant être reçus urgemment vers d'autres hôpitaux. Cette violation de données a également empêché le personnel d'avoir accès à leurs messageries électroniques pendant plus d'une semaine, et il a fallu plusieurs jours pour que le logiciel qui permette l'accès aux dossiers des patients soit de nouveau opérationnel (à 95%) suite à cette violation, ce qui a perturbé la continuité des soins à travers l'indisponibilité du matériel nécessaire au bon fonctionnement de l'hôpital. Le niveau de dommage retenu est donc modéré.

165. *Troisièmement,* s'agissant de la durée de la violation, la Chambre contentieuse rappelle que la durée de la violation dont il est question n'est pas relative à la durée de

[47] CEPD, Lignes directrices 01/2021 sur les Exemples concernant la notification de violations de données à caractère personnel (v2), adoptées le 14 décembre 2021 et disponibles sur le lien suivant : https://www.edpb.europa.eu/system/files/2022-09/edpb_guidelines_012021_pdbnotification_adopted_fr.pdf. S'agissant de l'indisponibilité temporaire de données comme forme de violation de données : « Par conséquent, un incident de sécurité entraînant l'indisponibilité temporaire de données à caractère personnel est également considéré comme un type de violation, dès lors que la perte de l'accès aux données peut avoir une incidence significative sur les droits et libertés des personnes physiques » (page 9).

[48] Conformément au considérant 75 du RGPD, le niveau de dommage renvoie aux dommages physiques, matériels ou à un préjudice moral.

la violation de données ou de ses conséquences dommageables, telle que décrite au paragraphe précédent. En effet, les mesures techniques et organisationnelles de l'hôpital auraient dû être en place depuis l'entrée en vigueur du RGPD le 25 mai 2018, et a minima depuis la première violation de données du [date] 2019. La durée de la violation est retenue à partir de ce dernier événement, et jusqu'à la violation de données de septembre 2021, laquelle marque le début des efforts de mise en conformité des mesures de sécurité, soit 2 ans et 6 mois. Il s'agit d'une durée modérée.

Caractère délibéré ou négligent de la violation (article 83, paragraphe 2, point b) du RGPD)

166. On distingue la violation causée par négligence de la violation causée délibérément. Le caractère délibéré d'une violation implique la rencontre de deux conditions, à savoir la connaissance d'une violation ainsi que la volonté de l'engendrer. La négligence se définit, au contraire, par l'absence de caractère intentionnel dans la réalisation de l'infraction, bien que le principe de diligence n'ait pas été respecté.

167. La Chambre contentieuse précise qu'un seuil élevé est fixé pour considérer une violation comme étant délibérée. De surcroît, la négligence peut également être appréciée par degrés.

168. En l'espèce, il ne ressort pas d'intentionnalité dans les manquements commis. Toutefois, eu égard au fait que les traitements de données sensibles constituent l'activité de base de la défenderesse, et que la défenderesse avait déjà subi une violation de données, la Chambre contentieuse considère que la défenderesse a commis une négligence sérieuse. Ce critère renforce la gravité de la violation.

Catégories de données à caractère personnel concernées par la violation (article 83, paragraphe 2, point g) du RGPD)

169. Il ressort des pièces du dossier que des données à caractère sensible dont le régime de protection est assuré par l'article 9 du RGPD, notamment des données de santé, sont concernées par la violation. La violation de ces catégories de données renforce la gravité de la violation.

Classification de la gravité de la violation et fixation du montant de départ adéquat

170. L'appréciation des éléments ci-dessus – à savoir la nature, gravité et durée de la violation, ainsi que le caractère délibéré ou négligent de la violation et les catégories de données à caractère personnel concernées – permet de déterminer le degré de

gravité de la violation dans son ensemble. Selon cette évaluation, la gravité de la violation peut être qualifiée de « faible », « moyenne » ou « élevée ».

171. En l'espèce, il y a tout d'abord lieu de relever que la violation de l'article 5 du RGPD figure parmi les violations listées à l'article 83.5 du RGPD, tombant ainsi sous le coup du niveau supérieur de l'article 83 du même Règlement.

172. Les traitements de données sensibles en cause concernent la gestion des dossiers médicaux de personnes vulnérables (patients) et les messages électroniques du personnel hospitalier, essentiels pour la continuité des soins. De plus, il apparaît que 300 000 patients figurent dans les bases de données de l'hôpital et que les employés de l'hôpital sont également concernés par la violation de données.

173. Cependant, le niveau de dommage avéré reste relativement modéré, avec une indisponibilité des messages électroniques du personnel pendant 12 jours, l'indisponibilité des dossiers médicaux informatisés pendant 3 jours, et la perturbation du service d'urgence pendant 3 jours comme principaux impacts démontrés.

174. En tout état de cause, la violation commise par la défenderesse trouve sa source dans une négligence sérieuse de la part de celle-ci, d'autant que l'hôpital a subi une première violation de données en 2019. La plupart des mesures de sécurité qui ont été mises en place après la seconde violation de données auraient dû être mises en place depuis l'entrée en vigueur du RGPD.

175. À la lumière des éléments exposés ci-avant, la Chambre contentieuse conclut que la violation constatée est de gravité moyenne. Dès lors, pour le calcul du montant de l'amende, il sera fixé un montant de départ compris entre 10% et 20% du montant maximum légal de 20 000 000 EUR prévu à l'article 83.5 du RGPD[49], c'est-à-dire entre 2 000 000 et 4 000 000 EUR.

176. **Au vu de ces éléments, la Chambre contentieuse décide de fixer un montant de départ à 15% du montant maximum légal prévu, soit 3 000 000 EUR.**

[49] CEPD - Lignes directrices 04/2022 sur le calcul des amendes administratives au titre du RGPD, adoptées le 24 mai 2023 (v2.1), disponible sur le site https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-042022-calculation-administrative-fines-under_fr, voir point 60

iii. Chiffre d'affaires du responsable de traitement et considérations supplémentaires prises en compte par la Chambre contentieuse pour déterminer le montant de l'amende[50]

177. Le RGPD exige de chaque autorité de contrôle qu'elle veille à ce que les amendes administratives imposées soient effectives, proportionnées et dissuasives dans chaque cas d'espèce (article 83.1 du RGPD).

178. Pour y parvenir, les autorités de contrôle devraient appliquer la définition de la notion d'entreprise telle qu'adoptée par la Cour de justice de l'Union européenne (ci-après « CJUE ») aux fins des articles 101 et 102 du TFUE, à savoir que la notion d'entreprise s'entend comme une unité économique qui peut être constituée par la société mère et toutes les filiales concernées. Conformément au droit et à la jurisprudence de l'UE, une entreprise doit donc être considérée comme une unité économique exerçant des activités commerciales/économiques, quelle que soit sa forme juridique[51]. L'objectif est d'assurer que les sanctions sont adaptées à la taille et à la puissance économique de l'entreprise.

179. Les autorités de contrôle sont censées ajuster les amendes administratives en fonction de la gravité de la violation, tout en respectant la fourchette prévue dans les lignes directrices de l'EDPB jusqu'au montant maximal légal. Cela peut conduire à des majorations ou des minorations significatives de l'amende, selon les circonstances du cas d'espèce.

180. En outre, les articles 83.4, 83.5 et 83.6 du RGPD prévoient que le chiffre d'affaires annuel mondial total de l'exercice précédent doit être utilisé pour le calcul de l'amende administrative. À cet égard, le terme « précédent » doit être interprété conformément à la jurisprudence de la CJUE en matière de droit de la concurrence, de sorte que l'événement pertinent pour le calcul de l'amende est la décision de l'autorité de contrôle relative à l'amende, et non le moment de l'infraction sanctionnée.

181. Comme rappelé au paragraphe 160, le chiffre d'affaires de la défenderesse est établi à (.. EUR) pour l'année 2023. Ce chiffre ressort des comptes annuels de l'ASBL Y (numéro d'entreprise : [...]) tels que déposés auprès de la Banque nationale de Belgique (BNB) le [date] 2024.

---

[50] CEPD - Lignes directrices 04/2022 sur le calcul des amendes administratives au titre du RGPD, adoptées le 24 mai 2023 (v2.1), disponible sur le site https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-042022-calculation-administrative-fines-under_fr, voir points 63 à 69 ; 112 à 131.

[51] La jurisprudence de la Cour de justice des Communautés européennes donne la définition suivante : "*la notion d'entreprise couvre toute entité exerçant une activité économique, indépendamment de son statut juridique et de son mode de financement*" (affaire C41/90, *Höfner et Elser/Macrotron*, ECLI:EU:C:1991:161, point 21). La notion d'entreprise " *doit être comprise comme désignant une unité économique, même si cette unité économique est constituée, d'un point de vue juridique, par différentes personnes physiques ou morales* " (affaire C-217/05, *Confederación Española de Empresarios de Estaciones de Servicio*, ECLI:EU:C:2006:784, point 40). ; CJUE, 10 septembre 2009, C-97/08 P, *Akzo Nobel nv et al. t. Commission*, ECLI:EU:C:2009:536), marges 60-61.

182. La Chambre contentieuse peut envisager d'ajuster le montant de départ en fonction du chiffre d'affaires annuel de l'entreprise[52]. Pour les entreprises dont le chiffre d'affaires annuel est compris entre 50 et 100 millions d'EUR, les lignes directrices sur le calcul des amendes permettent de procéder à un ajustement des calculs sur la base d'une somme comprise entre 8 % et 20 % du montant de départ fixé.

183. En l'espèce, la Chambre contentieuse décide de procéder à un ajustement de la somme de 3 000 000 EUR à hauteur de 13% du montant de départ fixé, soit 390 000 EUR. Ce calcul tient compte de la réduction de la durée de violation annoncée à la défenderesse dans le formulaire de sanction. Le montant de départ était en effet initialement de 400 000 EUR et est porté à 390 000 EUR pour tenir compte des arguments avancés par la défenderesse dans ses réponses au formulaire de sanction.

184. **Compte tenu des développements qui précèdent, la Chambre contentieuse décide concrètement de fixer le montant de départ pour la catégorie d'infractions à 390 000 EUR.**

iv. Circonstances aggravantes ou atténuantes

185. Compte tenu de l'article 83 du RGPD, la Chambre contentieuse doit également motiver l'imposition d'une amende administrative en des termes concrets, en tenant compte d'autres circonstances aggravantes ou atténuantes énumérées à l'article 83.2 du RGPD :

Mesures prises pour atténuer le dommage (article 83.2.c) du RGPD)

186. Comme rappelé par les lignes directrices du CEPD concernant le calcul des amendes administratives au titre du RGPD, « les responsables du traitement et les sous-traitants sont déjà tenus de «mettre en œuvre les mesures techniques et organisationnelles afin de garantir un niveau de sécurité adapté au risque, d'effectuer des analyses d'impact relatives à la protection des données et d'atténuer les risques pour les droits et les libertés des personnes résultant du traitement des données à caractère personnel». Toutefois, lorsqu'une violation a lieu, le responsable du traitement ou le sous-traitant «devrait faire tout ce qui est en son pouvoir pour réduire les conséquences de la violation pour la personne concernée »[53].

[52] CEPD - Lignes directrices 04/2022 sur le calcul des amendes administratives au titre du RGPD, voir point 66.

[53] CEPD - Lignes directrices 04/2022 sur le calcul des amendes administratives au titre du RGPD, voir point 74.

187. À ce titre, la Chambre contentieuse retient que :

- S'agissant de la perturbation du service des urgences : le Plan d'Urgence Hospitalier a été activé, permettant ainsi de rediriger les patients vers d'autres hôpitaux.
- S'agissant de l'impossibilité d'accéder aux messageries électroniques : l'hôpital a mis un « Patch » pour résoudre la faille du serveur Exchange et empêcher qu'une telle intrusion ne se reproduise.
- S'agissant du vol potentiel de données sensibles : l'hôpital a désactivé directement les liaisons vers et depuis l'extérieur afin de limiter l'étendue de l'attaque.
- S'agissant de l'indisponibilité du logiciel contenant les dossiers médicaux : la défenderesse a mis en place des outils de restauration afin de rétablir progressivement les systèmes de l'hôpital. Trois jours après l'attaque, le logiciel de gestion des dossiers médicaux était opérationnel à 95%.

188. La Chambre contentieuse retient que des mesures ont été prises pour atténuer le dommage. Ce critère constitue une circonstance atténuante.

Contexte sanitaire à l'époque de la violation (article 83.2.k) du RGPD)

189. Le contexte sanitaire à l'époque de la violation, le [date] 2021, est pris en compte dans la détermination du montant de l'amende. En pleine crise de la COVID-19, l'hôpital était confronté à une situation exceptionnelle, nécessitant une concentration accrue sur la dispensation des soins aux patients. Cette crise majeure a pu limiter les ressources et l'attention disponibles pour assurer pleinement la conformité aux exigences du RGPD. Ce critère constitue une circonstance atténuante.

Crise énergétique et inflation (article 83.2.k) du RGPD)

190. Il convient de tenir compte des circonstances économiques exceptionnelles auxquelles les hôpitaux sont confrontés. En effet, la crise énergétique et la hausse rapide de l'inflation ont entraîné une augmentation significative des coûts d'exploitation, ce qui exerce une pression financière accrue sur les ressources de l'hôpital. Ces facteurs impactent directement sa capacité à investir dans des mesures de sécurité renforcées pour la protection des données. Conformément à l'article 83.2.k) du RGPD, il est donc légitime de considérer cette conjoncture défavorable comme une circonstance atténuante, justifiant un ajustement de l'amende afin de ne pas compromettre davantage l'équilibre financier de l'hôpital et de permettre la continuité de ses missions dans des conditions difficiles.

191. En dépit des autres propositions formulées par la défenderesse invitant la Chambre contentieuse à considérer différemment le degré de gravité de la violation, ainsi qu'une autre interprétation des circonstances aggravantes et atténuantes applicables, la Chambre contentieuse décide de maintenir son analyse des circonstances aggravantes et atténuantes telle que retenue initialement dans le formulaire de sanction, à une exception[54]. En effet, la Chambre contentieuse a décidé de tenir compte de la crise énergétique et l'inflation envisagée comme nouvelle circonstance atténuante. Elle a tenu compte de cette modification pour adapter le montant final de l'amende.

v. Caractère effectif, proportionné et dissuasif

192. Les lignes directrices de l'EDPB rappellent que l'amende administrative prononcée pour les violations du RGPD visées à l'article 83.4 à 83.6 doit être effective, proportionnée et dissuasive dans chaque cas spécifique. Les autorités de contrôle doivent vérifier si le montant répond à ces critères et ajuster si nécessaire.

▪ Effectivité

193. Une amende est jugée effective si elle atteint les objectifs pour lesquels elle a été imposée, tels que restaurer le respect des règles, sanctionner les comportements illicites ou les deux.

194. En l'espèce, l'amende vise à sanctionner le comportement négligent et grave de la défenderesse. De plus, elle vise à dissuader d'autres violations similaires à l'avenir. La durée prolongée de la violation, malgré une première violation de données subie en 2019, démontre la nécessité d'une réponse ferme de la part de la Chambre contentieuse. Ainsi, l'imposition d'une amende administrative d'un montant de départ de 390 000 EUR constitue une mesure effective pour atteindre ces objectifs.

▪ Proportionnalité

195. Le principe de proportionnalité, tel que défini par le RGPD, énonce que les mesures adoptées ne doivent pas dépasser ce qui est approprié et nécessaire pour atteindre les objectifs légitimes de la réglementation en question. Dans le cas des amendes, cela signifie que leur montant ne doit pas être disproportionné par rapport aux buts visés, à la gravité de la violation, ainsi qu'à la taille et à la capacité financière de

[54] CEPD - Lignes directrices 04/2022 sur le calcul des amendes administratives au titre du RGPD, adoptées le 24 mai 2023 (v2.1), disponible sur le site https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-042022-calculation-administrative-fines-under_fr, voir point 6.

l'entreprise concernée. Par conséquent, les autorités de contrôle doivent donc s'assurer que le montant de l'amende soit proportionné à la violation appréciée dans son ensemble, en tenant compte de divers facteurs tels que la capacité financière de l'entreprise à payer.

196. Dans certaines circonstances exceptionnelles, une minoration de l'amende peut être envisagée si l'imposition de celle-ci mettrait irrémédiablement en danger la viabilité économique de l'entreprise concernée. Cette possibilité est envisageable lorsque des preuves objectives démontrent une incapacité de paiement. De plus, il est essentiel d'analyser les risques en considérant le contexte social et économique spécifique.

197. Dans le cas d'espèce, plusieurs critères indiquent que l'amende proposée est proportionnée :

- ***Viabilité économique et capacité financière de l'entreprise*** : Avec un chiffre d'affaires annuel consolidé de plus de 72 millions d'euros pour l'exercice 2023, la défenderesse dispose d'une capacité financière suffisante pour supporter une amende. Afin que l'amende proposée ne compromette pas la viabilité économique de l'hôpital, eu égard aux difficultés financières présentées par la défenderesse à l'appui de pièces dans son formulaire de sanction, la Chambre contentieuse consent une réduction de l'amende initialement prévue. En effet, même si le montant de départ de l'amende de 390 000 EUR ne représente qu'environ 0,54% d'un chiffre d'affaires (arrondi) de 72 000 000 EUR, ce montant doit être réduit d'environ un tiers en l'espèce pour tenir compte principalement (i) des difficultés financières de l'hôpital, en particulier l'aboutissement de son dossier de reconnaissance comme « Entreprise en difficulté » et la désignation d'un manager de crise, (ii) de la nouvelle circonstance atténuante retenue par la Chambre contentieuse, à savoir la crise énergétique et l'inflation, laquelle a également un impact sur la capacité financière de l'entreprise.

- ***Preuve de la perte de valeur*** : Aucune indication ne laisse présager que l'imposition de l'amende telle que révisée mettrait en danger la viabilité de l'entreprise, entraînant une perte significative de la valeur de ses actifs ou menaçant sa capacité à poursuivre ses activités de manière viable. Il doit y avoir un lien direct entre l'amende et cette perte de valeur, et il n'est pas automatiquement admis que la faillite ou l'insolvabilité conduisent à une telle perte, au vu du montant de l'amende révisé. En l'absence de telles preuves tangibles démontrant cette corrélation, une minoration supplémentaire de l'amende ne paraît pas justifiée.

- ***Contexte social particulier*** : Le contexte social de l'époque, marqué par la crise sanitaire de la COVID-19 en 2021, constitue un élément pris en considération par la Chambre contentieuse dans la détermination du montant de l'amende à infliger.

▪ **Dissuasion**

198. Le caractère dissuasif de l'amende doit revêtir deux dimensions. Elle doit dissuader la personne contre laquelle l'amende est infligée de réitérer les violations constatées à l'avenir, mais également toute autre personne de reproduire les comportements infractionnels commis par la première.

199. Plusieurs facteurs déterminent le caractère dissuasif d'une amende : la nature, le montant de l'amende et la probabilité de son imposition, sont des éléments déterminants à cet égard. Une amende doit être suffisamment élevée pour avoir un impact financier significatif sur l'entreprise fautive, tout en restant proportionnée à la gravité de la violation. En d'autres termes, le critère de la dissuasion recoupe celui de l'effectivité.

200. Si une autorité de contrôle estime qu'une amende n'est pas suffisamment dissuasive, elle peut envisager de la majorer. Dans certains cas, elle peut même appliquer un multiplicateur de dissuasion pour renforcer son effet dissuasif. Ce multiplicateur peut être ajusté à la discrétion de l'autorité de contrôle afin de garantir que les objectifs de dissuasion sont pleinement atteints.

201. **En l'espèce, compte tenu de la réévaluation de la durée de la violation, de la nouvelle circonstance atténuante prise en considération, ainsi que de la capacité financière de l'hôpital, le montant final de l'amende sera donc réévalué définitivement à 200.000 EUR.**

202. Ce montant reste suffisamment dissuasif pour empêcher la défenderesse de récidiver dans la violation des règles du RGPD. De plus, elle cherche également à dissuader d'autres entreprises de commettre des violations similaires. Cette amende, proportionnée à la gravité de la violation et tenant compte du chiffre d'affaires de la défenderesse, est conçue pour avoir un effet dissuasif à la fois spécifique et général.

III.3. Sur les ordres de mise en conformité

203. **Sur l'imposition d'une mesure de mise en conformité** : Les articles 58.2.d) du RGPD et 100§9 de la LCA permettent à la Chambre contentieuse d'ordonner au responsable du traitement de mettre les opérations de traitement en conformité avec les dispositions du RGPD, le cas échéant, de manière spécifique et dans un délai déterminé.

204. En l'espèce, la Chambre contentieuse considère que certaines mesures techniques et organisationnelles, ainsi qu'une AIPD, n'ont toujours pas été mises en place au jour de

la décision. La Chambre contentieuse ordonnera donc également à la défenderesse de se conformer aux ordres de mise en conformité énoncés au paragraphe suivant.

205. **Ordres de mise en conformité** : La Chambre contentieuse ordonne à la défenderesse de se conformer sur les points suivants dans un délai de 90 jours à compter de la notification de la décision :

a. Réaliser une analyse d'impact relative la protection des données, sur la base de l'article 35.3 du RGPD. La Chambre contentieuse rappelle que le contenu de cette AIPD doit reprendre a minima les conditions énoncées à l'article 35.7 du RGPD, dont une description systématique des traitements envisagés et les mesures envisagées pour faire face aux risques.

b. Mettre en place la « politique claire et précise relative à la sécurité de l'information et de la vie privée » (paragraphe 81 de la décision), conformément à la politique de sécurité de l'information du 3 mars 2022, pour garantir la sécurité des traitements mis en place par la défenderesse, conformément aux articles 5.1.f) et 32 du RGPD.

c. Mettre en place un programme de formation / sensibilisation des employés au RGPD régulier, afin que l'hôpital puisse s'assurer a minima que l'ensemble de son personnel connaisse les principes de base de traitement des données personnelles, dont le principe d'intégrité et de confidentialité. Cette exigence découle de l'application des articles 32, 5.1.f) et 24 du RGPD.

d. Renforcer la longueur du mot de passe d'accès au dossier informatisé du patient afin d'assurer la conformité aux articles 32, 5.1.f) et 24 du RGPD.

IV. Publication de la décision

206. 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 de la partie défenderesse soit directement communiquée.

PAR CES MOTIFS,

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

- **En vertu de l'article 58.2.d) du RGPD et de l'article 100§1, 9° de la LCA**, d'ordonner à la défenderesse, en raison de la violation des articles 35.3, 32, 5.1.f) et 24 du RGPD, de mettre les opérations de traitement en conformité avec les dispositions du RGPD.
- **En vertu de l'article 58.2.i) du RGPD et de l'article 100§1, 13° de la LCA**, lu conjointement avec l'article 101 de la LCA, imposer une amende administrative d'un montant de **200 000 EUR** à la défenderesse pour les violations des articles 35.3, 32, 5.1.f) et 24 du RGPD.
- D'ordonner à la défenderesse d'informer la Chambre contentieuse de la suite réservée à ces injonctions et ce au plus tard dans les 30 jours de la notification de ladite décision.

207. 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.

208. 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[55]. La requête interlocutoire doit être déposée au greffe de la Cour des marchés

---

[55] 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;

la signature du requérant ou de son avocat.

conformément à l'article 1034*quinquies* du C. jud.[56], 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

[56] 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.