Copie
Délivrée à: L'AUTORITE DE PROTECTION DES DONNEES
art. 792 CJ
Exempt du droit de greffe - art. 280,2° C.Enr.

Expédition

Délivrée à	Délivrée à	Délivrée à
le € CIV	le € CIV	le € CIV

Numéro du répertoire **2025 / 5578**
Date du prononcé **03 septembre 2025**
Numéro du rôle **2025/AR/74**

☒ Enregistrable

☐ Non enregistrable

Cour d'appel
Bruxelles

Section Cour des marchés
19e chambre A

Arrêt

Présenté le
Non enregistrable

COVER 01-00004516182-0001-0052-01-01-1

[redacted] (aussi couramment appelée « [redacted] »), enregistrée dans la Banque-Carrefour des Entreprises sous le numéro [redacted], dont le siège est établi à [redacted]

Partie requérante, ci-après aussi « [redacted] »,

représentée par Maître COTON Fanny, avocat dont le cabinet est établi à 1000 BRUXELLES, Rue Haute 139 bte 6 et par Maître RUELLE Victoria, [redacted]

CONTRE

L'AUTORITE DE PROTECTION DES DONNEES, enregistrée dans la Banque-Carrefour des Entreprises sous le numéro 0694.679.950, dont le siège est établi à 1000 BRUXELLES, Rue de la Presse 35,

Partie adverse, ci-après aussi « ***l'APD*** »,

représentée par Maître DEPRE Sébastien et Maître RYELANDT Grégoire, avocats dont le cabinet est établi à 1050 BRUXELLES, Place Eugène Flagey 18

***

Vu les pièces de la procédure, et notamment :

- l'arrêt interlocutoire du 19 février 2025 et les pièces y mentionnées, en particulier la décision n° 166/2024 quant au fond rendue le 17 décembre 2024 par la Chambre contentieuse de l'Autorité de protection des données (ci-après « **l'APD** ») dans le dossier DOS-2021-06114 (ci-après la « **Décision attaquée** » ou la « **Décision** ») ainsi que le recours en annulation contre ladite Décision déposé au greffe par la Requérante le 15 janvier 2025 ;
- les Conclusions visant l'annulation d'une décision de le Chambre contentieuse de l'APD déposées pour la Requérante le 4 avril 2025 ;
- les Conclusions synthèse déposées pour l'APD le 7 mai 2025 ;
- les pièces déposées par les parties.

Entendu les conseils des parties à l'audience publique du **21 mai 2025**.

I. Faits et antécédents procéduraux

1. Les faits et antécédents procéduraux ont été sommairement résumés comme suit dans l'arrêt interlocutoire :

> *« La Requérante, selon sa propre description, est une structure hospitalière située à [redacted] qui est composé d'un Hôpital et de [redacted] et fait partie du [redacted] Elle dispose de [redacted]*
>
> *Elle expose avoir fait l'objet d'une première attaque de pirates informatiques avec demande de rançon le 11 mars 2019, notifiée à l'APD et aux personnes concernées, à la suite de quoi elle dit avoir amélioré la sécurité de ses outils informatiques.*
>
> *Les 16 et 17 septembre 2021, elle fait l'objet d'une seconde attaque d'un pirate informatique avec demande de rançon. Elle notifie l'incident à l'APD et informe les personnes concernées via une note interne et un communiqué de presse.*
>
> *Le 20 octobre 2021, le Comité de Direction de l'APD demande au Service d'Inspection d'enquêter sur les pratiques de la Requérante.*
>
> *Le 22 novembre 2021 et le 11 février 2022, le Service d'inspection envoie au DPO de l'Hôpital des demandes d'informations, auxquelles celui-ci répond.*
>
> *Le 20 juin 2022, le Service d'Inspection transmet son rapport à la Chambre contentieuse de l'APD qui décide, le 27 septembre 2022, que le dossier peut être traité sur le fond, et l'invite à déposer ses conclusions écrites.*
>
> *Le 4 juillet 2024, la Chambre contentieuse organise une audition et entend la Requérante.*
>
> *Le 13 août 2024, la Chambre contentieuse informe la Requérante de son intention de lui imposer une amende administrative de 300.000,00 EUR. La Requérante adresse le 3 septembre 2024 à la Chambre contentieuse ses contestations.*
>
> *Le 17 décembre 2024, la Chambre contentieuse prononce la Décision attaquée ».*

2. Par l'arrêt interlocutoire du 19 février 2025, la Cour a débouté la partie Requérante de sa demande en suspension (partielle) de l'exécution de la Décision, et réservé à statuer pour le surplus.

II. La Décision attaquée

3. La Décision attaquée du 17 décembre 2024 examine les quatre constats de violation retenus par le rapport d'enquête du Service d'inspection et les considère établis :

- Constat n° 1 : manquement à l'obligation de réaliser une AIPD au sens de l'article 35.3. du RGPD (§ 72 de la Décision);
- Constat n° 2 : l'Hôpital 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 au moment de la violation des données (§ 88 de la Décision) ;
- Constat n° 3 : l'Hôpital 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 (§ 96 de la Décision) ;
- Constat n° 4 : sur les autres mesures de sécurité :
  - 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 (§ 105 de la Décision) ;
  - 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 (§ 113 de la Décision) ;
  - l'Hôpital 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 (§ 119 de la Décision) ;
  - l'Hôpital 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 aux dossiers informatisés de patients (§ 126 de la Décision).

Elle ordonne des mises en conformité et impose une amende administrative d'un montant de 200.000,00 EUR.

Son dispositif se lit comme suit :

> ***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.*

III. L'objet du recours

4. La **Requérante** sollicite par son recours l'annulation de la Décision, à titre subsidiaire la substitution de l'amende administrative et ordres de mise en conformité dans une seule sanction de réprimande, à titre infiniment subsidiaire, la réduction du montant de l'amende administrative à 1 EUR symbolique et à titre encore plus subsidiaire, que seul le plafond de l'amende prévu à l'article 83.4 du RGPD peut être pris comme point de départ du calcul de l'amende administrative.

Le dispositif de ses dernières conclusions se lit comme suit :

> – *Déclarer le recours recevable et fondé ;*
>
> – *À titre principal, l'Hôpital sollicite l'annulation de la décision quant au fond n° 166/2024 rendue le 17 décembre 2024 par la Chambre Contentieuse de l'APD dans le dossier DOS-2021-06114 ;*
>
> – *À titre subsidiaire, l'Hôpital sollicite que votre Cour fasse usage de son pouvoir de pleine juridiction et substitue à l'amende administrative et aux ordres de mise en conformité prononcés une seule sanction de réprimande ;*

- *À titre infiniment subsidiaire, la requérante sollicite que votre Cour fasse usage de son pouvoir de pleine juridiction et réduise le montant de l'amende administrative à 1 EUR symbolique ;*

- *À titre encore plus subsidiaire, l'Hôpital sollicite que seul le plafond de l'amende prévu à l'article 83.4 soit pris comme point de départ du calcul de l'amende administrative ;*

- *À tous les titres, condamner l'APD aux dépens, liquidés comme suit :*
  Frais de requête : 24 EUR
  Indemnité de procédure de base pour les litiges dont l'enjeu se situe entre 100.000 EUR et 250.000 EUR : 7.848,84 EUR
  Total : 7.872,84 EUR

5. L'**APD** demande la Cour :

Déclarer la demande recevable, mais non fondée ;

Condamner la requérante aux dépens, en ce compris l'indemnité de procédure au montant de base pour les litiges non évaluables en argent (1.883,72 €).

IV. Cadre juridique applicable

6. Le cadre légal applicable (ou potentiellement applicable) est constitué notamment des dispositions suivantes (sans exhaustivité) :

o *Le cadre légal européen applicable*

Le Règlement Général relatif à la Protection des Données (RGPD)[1]

[1] 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, *Pb.* L 119, 4 mai 2016.

- *Le cadre légal belge applicable*

Loi du 3 décembre 2017 portant création de l'Autorité de protection des données (ci-après « **LCA** »)[2] :

Article **4, §3**

Article **11**

Articles **15-16**

Articles **19-20**

Article **43**, **63** et **92**

Loi relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel :[3]

Article **5**

Article **221, §2**

V. Discussion

V.1. RECEVABILITE

7. La Décision attaquée a été prononcée par la Chambre contentieuse de l'APD le 17 décembre 2024.

Il n'est pas contesté que la requête a été déposée au greffe de la cour dans le délai de 30 jours visé à l'article 108, §1er, de la LCA.

Le recours est *recevable*.

[2] Dans la version applicable au litige, préalable à sa modification par la loi du 25 décembre 2023 modifiant la loi du 3 décembre 2017 portant création de l'Autorité de protection des données (*MB*, 1er mars 2024, entrée en vigueur le 1er juin 2024),

[3] Loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, *MB* 5 septembre 2018.

V.2. CONCERNANT LES MOYENS D'ANNULATION – FONDEMENT DU RECOURS

V.2.1. MOYENS DE LA REQUERANTE RELATIFS A LA REGULARITE FORMELLE DE LA DECISION

8. La Cour examinera ensemble les moyens 1 à 3 de la Requérante, concernant lesquels, dans un moyen introductif, **l'APD** invoque un défaut de juridiction de la la Cour des marchés, s'agissant d'actes du Secrétariat général ou du Comité de direction de l'APD, tandis que, selon la **Requérante**, en balayant les arguments procéduraux, la Chambre contentieuse a validé les différentes étapes qui l'ont conduite à examiner l'affaire et s'est appropriée la légalité (ou plutôt l'illégalité) des comportements antérieurs.

PREMIER MOYEN REQUERANTE : moyen pris de la violation des articles 11 et 92 de la LCA et des principes de bonne administration, de confiance légitime, ainsi que des articles 2 et 3 de la loi du 29 juillet 1991 relative à la motivation formelle des actes administratifs : l'APD ne pouvait utiliser les notifications de violations de données pour justifier la saisine du Service d'Inspection puis de la Chambre contentieuse.

Premier moyen APD.

La Requérante indique que ce moyen critique les §§ 26 à 34 et §§ 54 à 59 de la Décision attaquée.

Résumé des positions des parties

9. La **Requérante** fait valoir que ses notifications de violation de données faites à l'APD ne pouvaient pas déboucher sur la saisine de la Chambre contentieuse, cette hypothèse n'étant pas prévue par la LCA, ni par le RGPD lui-même. Il y a un vide juridique, qui n'a été comblé que dans le nouveau ROI de l'APD, non applicable en l'espèce.

L'action de l'APD a violé le principe de confiance légitime et les principes de sécurité juridique et de légalité, ainsi que du principe '*patere legem quam ipse fecisti*'. La Chambre contentieuse n'a pas été valablement saisie.

La Décision de l'APD viole aussi l'obligation de motivation ; elle ne permet pas de comprendre les raisons pour lesquelles la Chambre contentieuse n'a pas fait droit à la critique présentée par la Requérante

10. L'**APD** fait valoir dans un moyen introductif concernant les moyens 1 à 3 que la Cour des marchés n'a pas de juridiction pour statuer sur ces moyens qui critiquent des actes du Secrétariat général ou du Comité de direction.

Elle considère pour le surplus que la Décision attaquée est conforme aux articles 11 et 92 de la LCA, aux articles 2 et 3 de la loi du 29 juillet 1991, ainsi qu'aux principes de bonne administration et de confiance légitime. Le Secrétariat général n'est pas entré directement en relation avec le Service d'inspection, mais a uniquement transmis une information au Comité de direction, comme tous les départements de l'APD peuvent le faire. En ce qui concerne les autres normes visées au moyen, l'APD n'aperçoit pas en quoi elles seraient méconnues en l'espèce.

DEUXIEME MOYEN REQUERANTE : moyen pris de la violation des articles 19 et 20 de la LCA par la Chambre contentieuse : le Secrétariat général a outrepassé ses compétences lorsqu'il a analysé les notifications de violations de données et rendu son rapport au Comité de direction de l'APD.

Deuxième moyen APD.

Ce moyen critique les §§ 26 à 34 de la Décision attaquée.

Résumé des thèses des parties

11. Par son deuxième moyen, la **Requérante** soutient que le Secrétariat général a outrepassé ses compétences. Aucune tâche d'investigation ou de poursuite n'est confiée par le législateur au Secrétariat général et il n'a aucune compétence lui permettant d'analyser des notifications de violations de données ou d'instruire des dossiers spécifiques. Lorsque le Secrétariat général recommande au Comité de direction de transmettre le dossier au Service d'inspection, il s'agit à nouveau d'un outrepassement de compétences et la Cour des comptes a déjà critiqué sévèrement cette attitude du Secrétariat général. La référence à l'article 61 de la loi du 30 juillet 2018 par l'APD est erronée, car cet article se trouve dans le titre II de la loi relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel « par les autorités compétentes à des fins de prévention et de détection des infractions pénales (...) », non applicable en l'espèce. Ni le Secrétariat général ni le Comité de direction n'ont valablement saisi le Service d'inspection. Partant, la Chambre contentieuse ne saurait avoir été saisie valablement.

12. Outre son moyen d'incompétence général (cfr supra), l'**APD** conclut que la Décision attaquée est conforme aux articles 19 et 20 de la LCA. Nonobstant la note du Secrétariat général, c'est bien le Comité de direction qui a saisi le Service d'inspection, conformément à la LCA ; il n'a pas été 'contourné' par le Secrétariat général.

TROISIEME MOYEN REQUERANTE : moyen pris de la violation des articles 15 et 16 de la LCA et des principes de bonne administration : la décision du Comité de Direction ne respecte pas les règles qui régissent son adoption.
Troisième moyen APD.

Ce moyen critique les §§ 35 à 44 de la Décision attaquée.

Résumé des thèses des parties

13. La **Requérante** allègue que la transmission de la note du Secrétariat général aux membres du Comité de Direction n'est pas prouvée et l'absence du document dans le dossier constituait une violation des articles 15 et 16 de la LCA et des principes de bonne administration. En outre, décision du Comité de direction ne respecte pas les règles régissant son adoption et aurait dû être considérée comme nulle et non avenue : il n'y a pas de preuve que le quorum de présence était atteint, ni d'indication de la majorité à laquelle la décision a été prise concernant le point concerné (3.2.1.). Elle n'a donc pas valablement pu saisir le Service d'inspection et, partant, la Chambre contentieuse ne saurait avoir été saisie valablement.

14. Outre son moyen d'incompétence général (cfr supra), l'**APD** défend que la Décision attaquée est conforme aux articles 15 et 16 de la LCA et aux principes de bonne administration. En ce qui concerne les quorums, cet argument est déjà pleinement rencontré par la Décision attaquée (§38). La majorité des membres du Comité de direction étaient présents ce qui ressort de la formulation et de la mise en page de l'en-tête du PV de cette réunion et la décision du Comité de direction a été adoptée par consensus.

Discussion et décision quant à ces moyens 1 à 3

15. La procédure administrative à l'encontre de la Requérante trouve son origine dans sa notification d'une fuite de données à l'APD le 17 septembre 2021 (pièce 2 du dossier administratif), une notification complémentaire ayant été faite le 23 octobre 2021 (pièce 6 du dossier administratif), en raison d'une cyberattaque de type « ransomware » ayant touché le système informatique de la Requérante la nuit du 16 au 17 septembre 2021.

Le Secrétariat général a fait une note au Comité de direction à la suite de cette notification, lui suggérant de saisir le Service d'inspection sur la base de l'article 63, 1° LCA, au vu de possibles manquements à l'article 32 du RPGD (pièce 4 du dossier administratif). Lors de sa réunion du 20 octobre 2021, le Comité de direction a suivi cette suggestion et saisi le Service d'enquête (cfr pièce 2 de l'inventaire du dossier de pièces complémentaires de l'APD).

Les moyens 1 à 3 visent précisément l'origine de la procédure administrative, avant la saisine de la Chambre contentieuse : le fait que ce soit la notification d'une fuite de données qui ait déclenché

l'ouverture d'un dossier au sein de l'APD, le rapport fait par le Secrétariat général au Comité de direction, et enfin la régularité formelle de la décision du Comité de direction du 20 octobre 2021 de saisir le Service d'inspection.

La Chambre contentieuse n'a quant à elle été saisie du dossier que par le rapport d'enquête du Service d'inspection du 20 juin 2022 (pièce 14 du dossier administratif), conformément à l'article 91, § 1 et § 2 de la LCA.

16. Les articles 144 et 145 de la Constitution confient au ressort exclusif des cours et tribunaux les contestations qui ont pour objet des droits civils - à moins que la loi n'habilite le Conseil d'Etat ou les juridictions administratives fédérales à statuer sur les effets civils de leurs décisions - , et celles qui ont pour objet des droits politiques, sous réserve des exceptions établies par la loi.

Les cours et tribunaux n'ont pas de pouvoir de juridiction pour connaître des recours en annulation des actes des autorités administratives, sous réserve des cas prévus par les lois particulières.

C'est par l'effet de telles lois particulières que le législateur a conféré à la Cour des marchés la juridiction exclusive de connaitre de certains recours en annulation contre certaines décisions d'autorités administratives.

Dans le cas de l'APD, il s'agit de l'article 108 LCA. En vertu du § 1 de cette disposition, « *La chambre contentieuse informe les parties de sa décision et de la possibilité de recours dans un délai de trente jours, à compter de la notification à la Cour des marchés* ». En vertu du § 2 de cette disposition « *Un recours peut être introduit contre les décisions de la chambre contentieuse en vertu des articles 71 et 90 devant la Cour des marchés qui traite l'affaire selon les formes du référé conformément aux articles 1035 à 1038, 1040 et 1041 du Code judiciaire* », ce qui vise les décisions prises par la Chambre contentieuse dans le cadre de mesures provisoires (art. 70 et 71 de la LCA) et

Il ressort de cette disposition que le pouvoir de juridiction de la Cour des marchés est limité aux décisions de la Chambre contentieuse. La Cour n'a pas de pouvoir de juridiction pour connaitre des décisions prises par les autres organes de l'APD, que cela soit le Secrétariat général ou le Comité de direction.

17. L'absence de pouvoir de juridiction de la Cour des marchés ne signifie pas que la légalité de ces décisions ne peut pas être contestée. D'autres juridictions, administratives, peuvent être compétentes. En particulier le Conseil d'Etat est compétent, en vertu de l'article 14, § 1er, 1° des Lois coordonnées du 12 janvier 1973 sur le Conseil d'État pour statuer, « *Si le contentieux n'est pas attribué par la loi à une autre juridiction (...) sur les recours en annulation pour violation des formes soit substantielles, soit prescrites à peine de nullité, excès ou détournement de pouvoir, formés contre les actes et règlements: **1°** des diverses autorités administratives*; (...) », étant aussi précisé que « *Les irrégularités visées à l'alinéa 1er ne donnent lieu à une annulation que si elles ont été susceptibles*

d'exercer, en l'espèce, une influence sur le sens de la décision prise, ont privé les intéressés d'une garantie ou ont pour effet d'affecter la compétence de l'auteur de l'acte ».

L'article 78 du RGPD, qui prévoit le droit pour toute personne physique ou morale de former un recours juridictionnel effectif contre « *une décision juridiquement contraignante d'une autorité de contrôle qui la concerne* », réserve lui-même la possibilité de « *tout autre recours administratif ou extrajudiciaire* ».

Il résulte du considérant 143 du RGPD que les termes de « *décision juridiquement contraignante d'une autorité de contrôle* », visent en particulier une décision relative à « *l'exercice, par l'autorité de contrôle, de pouvoirs d'enquête, d'adoption de mesures correctrices et d'autorisation ou le refus ou le rejet de réclamations* ».

Les actes du Secrétariat général ou du Comité de direction critiqués par les moyens 1 à 3 de la Requérante peuvent donc faire l'objet d'un recours, à supposer les conditions de recevabilité d'un tel recours réunies devant le Conseil d'Etat. La Cour ne peut que constater que la Requérante n'a pas tenté d'exercer un tel recours.

Le fait que le législateur n'ait pas soumis toutes les décisions des organes de l'APD à un même recours – celui devant la Cour de marchés – n'est pas en soi critiquable et ne constitue pas une violation de l'article 78 du RGPD.

18. Le constat d'absence de juridiction qui précède n'est pas modifié par la circonstance que la Requérante a invoqué dans la procédure administrative devant la Chambre contentieuse les critiques qu'elle formule actuellement à l'encontre des décisions du Secrétariat général et du Comité de direction, avec pour conséquence que ces griefs ont été examinés (et rejetés) par la Chambre contentieuse dans la Décision attaquée.

Suivre l'argumentation de la Requérante reviendrait en effet à lui permettre de soumettre à la juridiction de la Cour des marchés la légalité de décisions pour lesquelles la Cour n'a pas reçu de compétence de la part du législateur. Par ailleurs, ce n'est pas la Chambre contentieuse qui est le juge de la légalité des actes posés par les autres organes de l'APD.

Au demeurant encore, les éventuelles irrégularités affectant les actes du Secrétariat général et du Comité de direction seraient en tout état de cause sans incidence sur la légalité de la Décision attaquée, qui clôt la procédure menée devant la Chambre contentieuse et dont celle-ci a été saisie par le Service d'inspection, après clôture de l'enquête, conformément à l'article 92, 3° LCA.

19. Il résulte de l'ensemble de ce qui précède que la Cour est sans juridiction pour connaitre des moyens 1 à 3 de la Requérante ou qu'en tout été de cause ces moyens ne sont pas fondés.

QUATRIEME MOYEN REQUERANTE : moyen pris de la violation de l'article 43 de la LCA et des principes de bonne administration et d'impartialité : le Président de la Chambre contentieuse a pris connaissance d'éléments concernant le dossier lors de la réunion du Comité de Direction et a ensuite connu à nouveau du dossier lorsqu'il l'a traité au fond.
Quatrième moyen APD.

Ce moyen critique les §§ 35 à 44 de la Décision attaquée.

Résumé des thèses des parties

20. La **Requérante** fait valoir une violation du principe d'indépendance et d'impartialité (article 43 de la LCA et principe général de bonne administration et d'impartialité) en ce que le Président de la Chambre contentieuse avait participé préalablement à la réunion du Comité de direction au cours de laquelle le Secrétariat général a rendu son rapport et recommandé la saisine du Service d'inspection, recommandation qui sera suivie par le Comité de direction. Rien n'établit que le Président de la Chambre contentieuse se serait abstenu de participer au vote sur ce point, le PV de la réunion ne le mentionnant pas. Le Président a donc pris connaissance d'éléments concernant la Requérante, alors qu'il a ensuite dû prendre position au fond à l'encontre de la Requérante. La Décision attaquée n'a donc pu valablement estimer que le Président de la Chambre contentieuse ne manquait pas d'impartialité et elle n'est pas motivée suffisamment. La décision de la Comité de direction n'a pas valablement pu saisir le Service d'inspection et, partant, la Chambre contentieuse ne saurait avoir été saisie valablement.

21. L'**APD** soulève que la Décision attaquée est conforme à l'article 43 de la LCA ainsi qu'aux principes de bonne administration et d'impartialité. Cet argument a déjà été présenté et écarté par la Chambre contentieuse (Décision, §39-43) et la Requérante ne démontre pas que la position de la Chambre contentieuse à cet égard n'est pas conforme aux principes applicables. Ce que la Requérante critique en réalité est l'organigramme et les procédures internes de l'APD, tels que prévus par la LCA. Or, la Cour des marchés n'est pas compétente pour écarter une norme législative. En tout état de cause, une violation du principe de bonne administration ne saurait entraîner automatiquement l'annulation de la Décision attaquée. La Requérante ne démontre en rien que, en l'absence de l'irrégularité qu'elle allègue, la Décision attaquée aurait été différente et que le Président de la Chambre contentieuse a pu exercer une influence déterminante sur les autres membres de l'organe collégial et en conséquence sur le sens de la décision adoptée.

Discussion par la Cour

22. Le grief de la Requérante invoque un manquement à l'impartialité (objective) du Président de la Chambre contentieuse, résultant de sa qualité de membre du Comité de direction de l'APD et de sa participation à ce titre à la réunion de cet organe du 20 octobre 2021, et sa prise de connaissance à cette occasion du rapport du Secrétariat général comportant certaines informations relatives à la Requérante, avant la saisine de la Chambre contentieuse.

Le principe d'impartialité s'applique à la Chambre contentieuse, vu sa qualité d'autorité administrative ; il s'agit d'un principe général de droit à valeur législative[4].

Le principe d'impartialité structurelle, selon lequel les membres d'un organe administratif qui ont mené l'enquête et proposé une sanction ne peuvent pas, en principe, participer à la décision sur le fond, ne s'applique que si cette application est compatible avec la nature inhérente, en particulier la structure inhérente, de l'autorité administrative et ne va donc pas à l'encontre d'une règle de droit claire (Cass. 6 novembre 2023, C.23.0092.N, concl. H. Vanderlinden, sur juportal.be). Le principe d'impartialité prescrit à l'autorité de s'organiser de manière à éviter de susciter chez l'administré une crainte légitime de partialité (impartialité objective) et lui interdit d'exprimer un quelconque parti pris ou préjugé à l'occasion de l'adoption d'un acte administratif (impartialité subjective)[5].

L'article 43 de la LCA est étranger aux circonstances de l'espèce, la Requérante n'alléguant pas que le Président de la Chambre contentieuse aurait eu un intérêt personnel ou direct au dossier ; l'intérêt ou incompatibilité qu'elle invoque est de type fonctionnel.

23. La participation du Président de la Chambre contentieuse au Comité de direction de l'APD, en ce compris la prise de connaissance des éléments soumis à ce Comité, n'est pas contraire au principe d'impartialité objective. Le Comité de direction ne mène en effet pas lui-même l'enquête, mais se contente d'examiner *prima facie*, l'existence d'indices sérieux de pratiques problématiques au niveau de la protection des données personnelles, et de charger le cas échéant le Service d'inspection d'enquêter sur celles-ci, conformément à l'article 63, 1° LCA.

Il n'apparaît par ailleurs aucunement que le Président de la Chambre contentieuse et membre à ce titre du comité de direction, ait joué un rôle particulier à l'occasion de la réunion du 20 octobre 2021.

Son intervention résulte du fonctionnement de l'APD et de son comité de direction tel qu'organisés par la LCA, dans sa version applicable à l'époque considérée. Comme rappelé par la Cour de

[4] Cfr not. Cass. 9 janvier 2002, P.00.0855.F, *JT*, 2002, p. 604 ; Cass. 6 novembre 2023, C. 23.0092.N. A. Daout et M. Dekleermaker, « Impartialité, indépendance et scrutin secret : 'principes' et applications », in *Les principes généraux de droit administratif*, Conférence du Jeune Barreau, Larcier, 2017, p. 567 et s.
[5] Cfr notamment A. Daout et M. Dekleermaker, *ibidem*.p. 567 et s.

cassation, le principe d'impartialité de l'administration ne peut pas être invoqué pour critiquer des actes posés conformément à l'organisation de l'organe d'administration prévue par la loi, en l'occurrence par la LCA (Cass. 6 novembre 2023, C.23.0092.N).

L'article 12 de la LCA, dans sa version applicable[6], dispose que « *Le comité de direction est composé du secrétariat général, du directeur du centre de connaissance, du directeur du service de première ligne, de l'inspecteur général et du président de la chambre contentieuse* ». Partant, le double rôle du Président de la Chambre contentieuse, comme président de cette chambre et membre du comité de direction, est directement et clairement prévu par la loi. Il n'est pas critiquable devant la Cour, et ce même si, contrairement à la pratique suivie dans d'autres dossiers, il n'est pas établi en l'espèce que le Président de la Chambre contentieuse se serait abstenu de prendre part à la délibération relative à l'envoi du dossier au service d'inspection pour enquête.

Comme l'indique le Conseil d'Etat, « *le principe général d'impartialité doit être compatible avec la structure de l'administration active (...)* »[7], ce qui implique que le principe d'impartialité ne peut conduire à restreindre trop fortement les choix liés à l'organisation de l'administration.

La circonstance que la procédure administrative à l'encontre de la Requérante ait trouvé son origine dans une Notification d'une fuite de données émanant de la Requérante elle-même ne modifie en rien l'analyse qui précède.

Enfin, la Décision de la Chambre contentieuse est régulièrement motivée en ce qu'elle ne retient pas le grief lié à la partialité de son Président (cfr § 39 à 44 de la Décision).

Le moyen n'est pas fondé.

[6] Article supprimé dans la version actuelle de la loi, après entrée en vigueur de la loi du 25 décembre 2023. La règle résulte actuellement de l'article 7, alinéa 2 de la LCA, en vertu duquel « chaque organe interne » de l'APD est dirigé par un membre différent du comité de direction, combiné avec l'article 8,§1, alinéa 1, qui dispose que l'APD est dirigée par un comité de direction composé de cinq membres.
[7] C.E., arrêt du 17 mai 2016, n° 234.744, en cause Del Pero.

CINQUIEME MOYEN REQUERANTE : moyen pris de la violation de l'article 63 de la LCA par la Chambre contentieuse, de l'erreur manifeste d'appréciation, du principe de sécurité juridique et des articles 2 et 3 de la loi du 29 juillet 1991 relative à la motivation formelle des actes administratifs : la Chambre contentieuse a commis une erreur manifeste d'appréciation et viole son obligation de motivation lorsqu'elle considère que le Comité de direction a valablement saisi le Service d'inspection sur la base d'indices sérieux de l'existence d'une pratique susceptible de donner lieu aux principes fondamentaux de la protection des données à caractère personnel, notamment en se fondant sur des éléments erronés.
Cinquième moyen APD.

Ce moyen critique les §§ 45 à 53 de la Décision attaquée.

Résumé des thèses des parties

24. Par son cinquième moyen, la **Requérante** fait valoir que la Chambre contentieuse n'a pas agi comme une autorité administrative normalement prudente et diligente et qu'elle a commis une erreur manifeste d'appréciation, parce qu'elle aurait dû vérifier que les indices sérieux de violation ayant justifié la saisine du Service d'inspection étaient avérés. Les faits repris au titre des indices sérieux par le Secrétariat général et le Comité de Direction étaient en partie inexacts et ont été contestés par la Requérante tout au long de la procédure. Il n'y avait pas d'indices sérieux de violation. A tort, la Chambre contentieuse n'a pas examiné la conséquence de cette erreur de motivation sur la validité de la décision du Comité de direction. Ainsi, la Décision attaquée est motivée par des éléments incorrects en fait ou à tout le moins incomplets. Reposant sur une motivation inexacte, la Décision attaquée doit être annulée.

25. L'**APD** soutient premièrement que la Cour n'a pas de juridiction pour statuer sur le cinquième moyen de la Requérante. Deuxièmement, l'APD fait valoir que l'ensemble des considérations relayées par la Requérante sont rencontrées par la Décision attaquée (§48-53). En outre, la Requérante confond le rôle du Comité de direction (qui statue sur l'existence d'indices sérieux) lorsqu'il décide de soumettre un dossier au Service d'inspection avec le rôle du Service d'inspection lui-même (qui établit des faits). Au surplus, même au regard de la version établie par le Service d'inspection, l'appréciation initiale du Comité de direction ne semble pas manifestement déraisonnable et la décision du Comité de direction de saisir le Service d'inspection est dument motivée par référence.

Discussion par la Cour

26. La Cour constate que le moyen critique en réalité l'appréciation par le Comité de direction des « indices sérieux » au sens de l'article 63, 1° LCA justifiant la saisine du Service d'inspection.

Comme indiqué ci-avant dans l'examen des moyens 1 à 3, la Cour n'a pas de juridiction pour connaitre d'un recours contre une décision du Comité de direction, et n'est pas l'organe compétent pour connaitre des critiques concernant une telle décision.

Ce constat d'absence de juridiction n'est pas modifié par la circonstance que la Requérante a invoqué dans la procédure administrative devant la Chambre contentieuse les critiques qu'elle formule actuellement à l'encontre de la décisions du Comité de direction, avec pour conséquence qu'elle formule actuellement ces critiques comme visant la Décision elle-même.

Suivre l'argumentation de la Requérante reviendrait en effet à lui permettre de soumettre à la juridiction de la Cour des marchés la légalité de décisions pour lesquelles la Cour n'a pas reçu de compétence de la part du législateur. Par ailleurs, ce n'est pas la Chambre contentieuse qui est le juge de la légalité des actes posés par les autres organes de l'APD.

Au demeurant encore, les éventuelles irrégularités affectant la décision du Comité de direction quant aux « indices sérieux » au sens de l'article 63, 1° LCA seraient en tout état de cause sans incidence sur la légalité de la Décision attaquée, qui clôt la procédure menée devant la Chambre contentieuse et dont celle-ci a été saisie par le Service d'inspection, après clôture de l'enquête, conformément à l'article 92, 3° LCA.

La Cour n'est donc pas compétente pour connaitre du moyen qui serait en tout état de cause non fondé.

SIXIEME MOYEN REQUERANTE : moyen pris de la violation de l'article 4, § 3 de la LCA : absence de signature de la Décision attaquée par les trois membres de la Chambre contentieuse.
Sixième moyen APD.

Résumé des parties

27. La **Requérante** fait valoir que selon l'article 4, §3, de la LCA, toute décision juridiquement contraignante de l'APD doit être signée. La Décision attaquée n'est signée que par le Président de la Chambre contentieuse, tandis qu'une décision prise en formation collégiale doit être signée par tous les membres ayant participé à la délibération, afin de garantir la légalité et la transparence de la décision. Le fait qu'elle ne soit signée que par le Président compromet le caractère collégial de la décision. Par conséquence les principes de collégialité, légalité, impartialité, transparence ainsi que

l'obligation de motivation sont violés. La signature unique constitue une irrégularité qui entache la légalité de la Décision.

28. L'**APD** soulève qu'il faut interpréter l'article 4, § 3, de la LCA à la lumière du considérant 129 du RGPD selon lequel il ressort qu'il est parfaitement envisageable que le Président signe seul les décisions prises par la Chambre contentieuse. C'est à tort que la Requérante évoque le principe de collégialité ; ce n'est pas parce que l'*instrumentum* de la Décision attaquée a été signé par le Président de la Chambre contentieuse que cela impliquerait que le *negotium* de celui-ci n'a pas été décidé de manière collégiale. Le moyen n'est donc pas fondé.

Discussion et décision par la Cour

29. L'article 4 § 3 LCA prévoit que :
« Toute décision juridiquement contraignante de l'Autorité de protection des données est datée, signée et motivée, et fait référence aux recours qui peuvent être introduits contre la décision ».

En vertu de cette disposition, qui s'applique à la Décision, celle-ci doit être signée. Il n'est pas précisé la qualité ni le nombre de signataires.

La Chambre contentieuse est un organe administratif de l'APD et en tant que tel, ne fait pas partie des cours et tribunaux de l'ordre judiciaire, comme précisé à l'article 4 § 2 de la LCA. Sa procédure est de type administratif et non juridictionnel. Le Code judiciaire ne lui est pas applicable.

La Cour relève qu'aucune disposition de la LCA ou du ROI de l'APD n'impose que les décisions de la Chambre contentieuse soient signées par d'autres personnes que son Président, en particulier par les autres membres ayant constitué le siège[8]. Il faut en déduire que le législateur a estimé que cette exigence n'était pas nécessaire, et c'est un choix qui lui appartient. Le RGPD n'impose pas non plus cette exigence, son considérant 129[9] se bornant à faire référence à la signature du « chef » de l'autorité nationale (ou d'un représentant autorisé), ce qui se traduit, dans le cas d'une décision de la Chambre contentieuse, par la signature de son Président.

Il n'y a pas non plus violation de la collégialité prévue par la LCA, même si les deux autres membres de la formation collégiale ne l'ont pas signée. En effet, leurs noms sont indiqués sur la Décision et la formulation de celle-ci fait bien apparaître que la Chambre contentieuse a pris la Décision en sa formation collégiale. Contrairement à ce que tente de faire valoir la Requérante, il n'existe pas de formule sacramentelle à cet égard, et notamment pas d'obligation pour le Président de la formation collégiale d'indiquer expressément qu'il signe pour la Chambre en formation collégiale.

[8] Cf l'arrêt de la Cour des marchés du 24 février 2021, 2020/AR/1159, pp. 15-16. Voir aussi l'arrêt de la Cour des marchés du 18 juin 2025, 2024/AR/2091, pp. 13-14.
[9] Ce considérant vient à l'appui de l'interprétation. Il n'est pas une source de droit lui-même.

L'accord des deux autres membres de la formation collégiale est implicite mais certain, et la Requérante ne rapporte d'ailleurs aucun élément qui en ferait douter.

La Décision attaquée, en ce qu'elle porte la seule signature du Président de la Chambre contentieuse est légale. Elle n'est pas non plus, du fait de la signature unique, contraire à un principe d'impartialité, de transparence – la transparence est bien assurée par la mention des noms de tous les membres de la formation collégiale - ou de motivation ou plus largement aux principes de bonne administration.

Le moyen n'est pas fondé.

V.2.2. MOYENS RELATIFS AUX CONSTATS DE MANQUEMENT FAITS PAR LA CHAMBRE CONTENTIEUSE

SEPTIEME MOYEN REQUERANTE : moyen pris des erreurs manifestes d'appréciation de la Chambre contentieuse et de la violation du principe de motivation des actes administratifs (loi du 29 juillet 1991 relative à la motivation formelle des actes administratifs) : la Chambre contentieuse ne tient pas compte et ne rencontre pas tous les arguments soulevés par l'Hôpital dans ses conclusions, des remarques adressées par l'Hôpital suite au PV de l'audience ni des mesures prises par l'Hôpital pour améliorer sa conformité aux prescrits du RGPD.
Septième moyen APD.

Résumé des thèses des parties

30. Par son septième moyen, la **Requérante** reproche à l'APD des erreurs manifestes d'appréciation, excès de pouvoir et des violations du principe de motivation. La Chambre contentieuse confirme les constats du Service d'inspection sans tenir compte des explications fournies par la Requérante dans ses conclusions et à l'audition.

La première branche du moyen critique les §§ 60 à 72 de la Décision attaquée. La Requérante fait valoir que la Chambre contentieuse viole les articles 2 et 3 de la loi du 29 juillet 1991 relative à la motivation formelle des actes administratifs et commet une erreur manifeste d'appréciation lorsqu'elle conclut que l'Hôpital a manqué à son obligation de réaliser une analyse d'impact (AIPD) pour les traitements de données concernés par l'attaque informatique. Elle commet aussi un excès de pouvoir lorsqu'elle sanctionne l'absence d'AIPD relative aux dossiers médicaux informatisés des patients.

En vertu de l'article 35, point 3, sous b, du RGPD et du raisonnement de la Chambre contentieuse, si une analyse d'impact avait dû être réalisée par la Requérante, cette analyse aurait dû porter uniquement sur les traitements à grande échelle de catégories particulières de données (données de santé et génétiques des patients). *En l'espèce*, ces traitements sont réalisés via les dossiers médicaux

informatisés des patients qui sont stockés sur le programme Omnipro hébergé sur des serveurs Linux. Or, ce programme et ces serveurs n'ont pas été visés par l'attaque et les traitements n'entrent pas dans les limites de l'enquête du Service d'inspection et de la saisine de la Chambre contentieuse. En statuant là-dessus, la Chambre contentieuse outrepasse sa saisine, commettant un excès de pouvoir. En plus, contrairement à ce que la Chambre contentieuse allègue dans la Décision attaquée, le RGPD n'impose pas de formalisme particulier au responsable du traitement qui veut réaliser une analyse d'impact. En tout cas, les risques de violation des données sont bien pris en compte par la Requérante et la Chambre contentieuse donc a commis une erreur manifeste d'appréciation lorsqu'elle estime que la Requérante n'a pas procédé à des analyses de risque des traitements des données réalisés.

La deuxième branche du moyen critique les §§ 76 à 88 de la Décision attaquée. La Requérante fait valoir dans celle-ci que la Chambre contentieuse viole les articles 2 et 3 de la loi du 29 juillet 1991 relative à la motivation formelle des actes administratifs et commet une erreur manifeste d'appréciation lorsqu'elle indique que l'Hôpital ne bénéficie pas d'une politique de sécurité des informations au moment de l'attaque.

Le RGPD n'impose pas expressément de disposer d'une politique de sécurité de l'information, ni *a fortiori* un quelconque formalisme pour une telle politique. Dès lors, non seulement l'infraction retenue par la Chambre contentieuse n'est pas adéquatement motivée, mais l'ordre de mise en conformité est également peu clair, et en tout cas sujet à appréciation de la part de l'APD. Par ailleurs, la Chambre contentieuse a commis une erreur manifeste d'appréciation en ne tenant pas compte de l'ensemble des politiques et procédures en place au sein de la Requérante.

La troisième branche du moyen critique les §§ 89 à 96 de la Décision attaquée. La Requérante fait valoir que la Chambre contentieuse viole les articles 2 et 3 de la loi du 29 juillet 1991 relative à la motivation formelle des actes administratifs et commet une erreur manifeste d'appréciation lorsqu'elle conclut à l'inefficacité de la politique et des procédures de mise à jour de sécurité des équipements informatiques de l'Hôpital.

La quatrième branche du moyen critique les §§ 97 à 105 de la Décision attaquée. La Requérante fait valoir que la Chambre contentieuse viole les articles 2 et 3 de la loi du 29 juillet 1991 relative à la motivation formelle des actes administratifs et commet une erreur manifeste d'appréciation lorsqu'elle conclut à l'absence d'un programme de formation/sensibilisation des employés.

L'infraction ne repose sur aucune exigence légale : en reprochant à la Requérante de ne pas avoir de 'véritable programme de formation continue et systématique au RGPD tel que requis par l'article 32 du RGPD', alors que cet article n'impose aucun programme de formation, la Décision attaquée n'est pas valablement motivée. Au demeurant, l'Hôpital forme bien son personnel. La Chambre contentieuse ne tient pas suffisamment compte du contexte particulier du travail en Hôpital (fortement chargé, Covid-19). De plus, une formation a été donnée au personnel concernant le plan

d'urgence hospitalier (e.g. scénario d'attaque informatique), certains membres ont participé d'initiative aux journées de simulations cyberattaques données par [redacted] etc. La Requérante a donc un véritable programme de sensibilisation de ses employés.
La Chambre contentieuse ne peut se contenter d'affirmer que le programme de formation mis en place par l'Hôpital n'est pas un véritable programme de sensibilisation continue et systématique au RGPD, sans expliquer concrètement ce qui aurait dû être mis en place.

La cinquième branche du moyen critique les §§ 106 à 113 de la Décision attaquée. La Requérante fait valoir que la Chambre contentieuse viole les articles 2 et 3 de la loi du 29 juillet 1991 relative à la motivation formelle des actes administratifs et commet une erreur manifeste d'appréciation lorsqu'elle considère comme une infraction l'absence d'un système de préservation des logs en vue d'analyses ultérieures lors d'incidents.

L'article 32, point 1, sous b, du RGPD n'impose pas textuellement de préservation des logs. La portée de l'obligation est différente pour chaque responsable du traitement et pour chaque traitement, puisqu'elle dépend de la mise en balance prescrite par le début de l'article 32, point 1, du RGPD.

La sixième branche du moyen critique les §§ 114 à 119 de la Décision attaquée. La Requérante fait valoir que la Chambre contentieuse viole les articles 2 et 3 de la loi du 29 juillet 1991 relative à la motivation formelle des actes administratifs et commet une erreur manifeste d'appréciation lorsqu'elle conclut à l'absence d'audits systématiques de la qualité de la sécurité des données à caractère personnel.

L'article 32, point 1, sous d, du RGPD 'propose' une série de mesures techniques et organisationnelles et n'impose pas de réaliser des audits périodiques, et *a fortiori* ne précise pas leur fréquence. De nouveau, la portée de l'obligation dépend de la mise en balance prescrite par le début de l'article 32, point 1, du RGPD. La Chambre contentieuse s'est abstenue de faire une mise en balance des risques et des moyens dont disposait la Requérante.

La septième branche du moyen critique les §§ 120 à 126 de la Décision attaquée. La Requérante fait valoir que la Chambre contentieuse viole les articles 2 et 3 de la loi du 29 juillet 1991 relative à la motivation formelle des actes administratifs, du principe des droits de la défense, d'*audi alteram partem* et commet une erreur manifeste d'appréciation lorsqu'elle retient une faible sécurisation du mot de passe d'accès au dossier informatisé du patient.

La Chambre contentieuse sanctionne la Requérante pour n'avoir pas utilisé suffisant de caractères pour ses mots de passes (6 à 8 caractères), sans avoir donné à la Requérante l'occasion de répondre à ce grief. La Chambre contentieuse viole ainsi le principe de bonne administration et d'*audi alteram partem*, de même que le principe des droits de la défense. Par ailleurs, la Chambre contentieuse n'a pas motivé adéquatement sa décision en estimant que cela constituait un manquement au RGPD, sans mettre en balance les risques et les moyens dont dispose la Requérante.

31. L'**APD** conclut au non-fondement du moyen.

Premièrement, l'APD fait valoir que même si la Requérante parvient à démontrer qu'une ou plusieurs AIPD ont été réalisées après septembre 2021, ces analyses, effectuées tardivement, n'ont pas d'incidence sur les constats d'infraction au RGPD relevés dans la Décision attaquée.

Deuxièmement, selon l'APD, la Requérante n'a pas démontré qu'elle disposait d'une politique de sécurité des informations formelle et actualisée au moment de l'attaque. La mise en place tardive d'une politique claire et précise relative à la sécurité de l'information et de la vie privée ne peut avoir aucune incidence sur les constats d'illégalité relevés dans la Décision attaquée.

Troisièmement, la Requérante a failli à son obligation de prévoir une politique et/ou une procédure de mise à jour de sécurité des équipements informatiques efficace au moment de la violation. Il n'appartient pas à la Chambre contentieuse d'expliquer quelles mesures auraient, concrètement, être pris ; le RGPD prévoit qu'il est de la responsabilité du responsable du traitement de démontrer que le traitement respecte les exigences prévues par l'article 5, § 1er.

Quatrièmement, la Requérante ne disposait pas d'un véritable programme de formation/sensibilisation des employés au RGPD. Elle ne démontre pas en quoi les arguments avancés par la Chambre contentieuse seraient entachés d'une illégalité. En ce qui concerne la nécessité de mettre en place un programme de formation continue et systématique au RGPD, cette obligation découle de la lecture combinée des articles 32.5, point 1, sous f) et 24 du RGPD. La comparaison entre les mesures concrètes mises en œuvre par la Requérante en matière de formation et les obligations découlant du RGPD met en évidence que le programme de sensibilisation tel qu'il existait avant l'incident était insuffisant et ne répondait pas aux standards requis.

Cinquièmement, la Requérante n'a pas mis en place les mesures adéquates pour préserver les logs contre des suppressions malveillantes ou le chiffrement, compromettant ainsi la capacité à analyser des violations de données. Il revient à la Requérante de démontrer en quoi les arguments avancés par la Chambre contentieuse dans la Décision attaquée seraient entachés d'une illégalité. Concernant la nécessité de mettre en place un système de journalisation permettant la préservation des logs en vue d'analyses ultérieures lors de violations de données, cette obligation découle de la lecture combinée des articles 32 ; 5, point 1, sous f) et 24 du RGPD.

Sixièmement, la Requérante a manqué à son obligation de sécurité en n'ayant pas mis en place des audits réguliers et systématiques pour tester l'efficacité des mesures techniques et organisationnelles au moment de la violation. Cette obligation découle de la lecture combinée des

articles 32, point 1, sous d), et 5, point 1, sous f), du RGPD. En outre, la Requérante est liée par les Normes minimales de sécurité de l'information et vie privée.

Finalement, la Requérante n'a pas respecté les critères prévus par les articles 32 ; 5, point 1, sous f), et 24 du RGPD car la robustesse du mot de passe qu'elle a implémentée n'était pas suffisante. La motivation de la Décision attaquée est adéquate et permet à la Requérante de comprendre le manquement qui lui est reproché.

Discussion et décision par la Cour

32. La première branche du moyen vise la Décision en ce qu'elle retient un constat n° 1 de violation, à savoir une violation de l'article 35.3 du RGPD pour défaut de réalisation d'une analyse d'impact relative à la protection des données (AIPD).

En vertu de l'article 35.1. du RGPD, « *Lorsqu'un type de traitement, en particulier par le recours à de nouvelles technologies, et compte tenu de la nature, de la portée, du contexte et des finalités du traitement,* ***est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques****, le responsable du traitement effectue,* ***avant le traitement, une analyse de l'impact des opérations de traitement envisagées sur la protection des données à caractère personnel****. Une seule et même analyse peut porter sur un ensemble d'opérations de traitement similaires qui présentent des risques élevés similaires* » (mise en évidence par la Cour).

En vertu de l'article 35.3. du RGPD, « *L'analyse d'impact relative à la protection des données (…) est en particulier requise dans les cas suivants : (…) b) le traitement à grande échelle de catégories particulières de données visées à l'article 9, paragraphe 1 (…)* ».

Les données de santé font partie des données visées à l'article 9, paragraphe 1 du RGPD, ce qui n'est pas contesté.

Par application de ces dispositions, la Requérante, en sa qualité de responsable de traitement traitant les données de santé de ses patients devait procéder à une AIPD conformément à l'article 35.1 du RGPD.

A bon droit, la Décision attaquée retient, à la suite du rapport d'enquête du Service d'inspection, une violation de cette disposition pour défaut de réalisation de cette AIPD.

33. La Requérante fait valoir que les dossiers médicaux informatisés des patients sont stockés sur le programme Omnipro, hébergé sur des serveurs Linux qui n'ont pas été touchés par la cyberattaque. Cette circonstance ne change cependant rien à l'obligation pour la Requérante d'effectuer une AIPD, et à son défaut de l'avoir fait. Il est inexact de soutenir que l'enquête n'aurait pas porté sur les données médicales des patients, la protection de ces données étant au cœur de

celle-ci (cfr notamment les questions n° 8 et 9 posées par le Service d'inspection au DPO de la Requérante ; cfr p. 11 et 12 du Rapport d'enquête, pièce 14 du dossier administratif).

Peu importe aussi que l'absence d'AIPD soit jugée par la Requérante comme ayant été sans impact sur la cyberattaque dont elle a été la victime.

La Requérante paraît ne pas comprendre que la cyberattaque dont elle a été l'objet, faisant suite à une précédente attaque survenue peu de temps avant, n'a été que l'élément qui a provoqué l'ouverture de l'enquête visant les mesures de sécurité qu'elle devait mettre en place conformément au RGPD.

A tort également, la Requérante tente-t-elle de faire valoir qu'elle n'aurait pas été soumise à l'obligation de réaliser une AIPD au motif qu'elle traitait déjà des données avant l'entrée en vigueur du RGPD. Il est erroné de soutenir que les traitements de données effectués par la Requérante seraient tous des traitements qui auraient été déjà existant à la date d'entrée en vigueur du RGPD.

34. Tout aussi vainement, la Requérante tente-t-elle de soutenir qu'elle aurait en réalité réalisé une telle AIDP, au motif qu'il n'existerait aucun prérequis formel pour une telle analyse, qu'elle aurait implicitement réalisé, ce qui ressortirait des différentes mesures de sécurité adoptées, et des analyses de ses sous-traitants informatiques.

En réponse à la question soulevée par le Service d'inspection, le DPO de la Requérante a répondu lui-même que « *Les analyses d'impact n'ont pas encore débuté mais sont prévues à partir de notre logiciel DPM de registre de traitement. Néanmoins, à la suite du hacking de 2019, des mesures ont été prises pour réduire les risques qui sont détaillées (...)* » (p. 10 du rapport d'enquête, réponse à la première question). Cette absence d'analyse d'impact est aussi reconnue par le DPO dans sa réponse aux questions 3 et 4.

Dans ses conclusions, la Requérante reconnait d'ailleurs qu'une analyse d'impact était prévue et devait être réalisée par PWC (cfr p. 53 de ses conclusions), ce dont il se déduit qu'effectivement, l'analyse d'impact n'avait pas encore été faite, ce que la Requérante savait parfaitement.

S'il n'existe pas de format précis à respecter, une analyse d'impact se matérialise en effet par un document dont il ressort qu'un audit a été réalisé quant aux risques pour la sécurité des données personnelles et quant aux mesures prises pour atténuer ce risque. Il s'agit d'une analyse à effectuer, préalablement au traitement, « *en vue d'évaluer la probabilité et la gravité particulière du risque élevé, compte tenu de la nature, de la portée, du contexte et des finalités du traitement et des sources du risque* » (cfr considérant 90 du RGPD) ; l'analyse doit aussi comprendre, notamment « *les mesures, garanties et mécanismes envisagés pour atténuer ce risque, assurer la protection des données à caractère personnel et démontrer le respect* » du RGPD (cfr considérant 90).

Enfin, même s'il faut saluer l'intention de la Requérante de se mettre en conformité (dans le futur), force est de constater qu'elle n'était pas en conformité lorsque l'enquête a été menée, alors que l'obligation de réaliser une AIPD est préalable aux traitements.

La Requérante n'établit aucunement qu'elle avait procédé à une telle analyse d'impact au moment de l'enquête et que la Décision procéderait d'une mauvaise application de l'article 35 du RGPD ou d'une erreur manifeste d'appréciation.

35. Il découle de l'ensemble de ce qui précède qu'en retenant le constat de violation n° 1 relatif à l'absence d'AIPD, la Décision attaquée n'a commis ni erreur d'appréciation, ni excès de pouvoir.

La Décision relative au constat de violation n° 1 est également adéquatement motivée, la motivation étant détaillée et adéquate (cfr § 60 à 72 de la Décision).

36. La deuxième branche du moyen vise la Décision en ce qu'elle retient un constat n° 2 de violation, à savoir une violation des articles 5.1.f et 32 du RGPD pour défaut de « politique de sécurité de l'information formelle et actualisée au moment de la violation des données» (Décision attaquée, § 88).

En vertu de l'article 5 « **Principes relatifs au traitement des données à caractère personnel** », « *1. Les données à caractère personnel doivent être: (...) f) traitées de façon à garantir une sécurité appropriée des données à caractère personnel, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées (intégrité et confidentialité)* ».

En vertu du paragraphe 2 de la même disposition, « ***Le responsable du traitement est responsable du respect du paragraphe 1 et est en mesure de démontrer que celui- ci est respecté*** *(responsabilité)* ».

L'article 32 RGPD dispose que:

« *1.**Compte tenu de l'état des connaissances, des coûts de mise en oeuvre et de la nature, de la portée, du contexte et des finalités du traitement** ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques, **le responsable du traitement et le sous-traitant mettent en oeuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque**, y compris entre autres, selon les besoins:*
a) la pseudonymisation et le chiffrement des données à caractère personnel;
b) des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement;
c) des moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique;

d)une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement.
2.Lors de l'évaluation du niveau de sécurité approprié, il est tenu compte en particulier des risques que présente le traitement, résultant notamment de la destruction, de la perte, de l'altération, de la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou de l'accès non autorisé à de telles données, de manière accidentelle ou illicite.
3.L'application d'un code de conduite approuvé comme le prévoit l'article 40 ou d'un mécanisme de certification approuvé comme le prévoit l'article 42 peut servir d'élément pour démontrer le respect des exigences prévues au paragraphe 1 du présent article.
4.Le responsable du traitement et le sous-traitant prennent des mesures afin de garantir que toute personne physique agissant sous l'autorité du responsable du traitement ou sous celle du sous-traitant, qui a accès à des données à caractère personnel, ne les traite pas, excepté sur instruction du responsable du traitement, à moins d'y être obligée par le droit de l'Union ou le droit d'un État membre ».

37. Dans sa réponse à la question du Service d'inspection « Politique de sécurité : - De quand date la version initiale de la politique de sécurité de l'information ? - Merci de nous communiquer les 3 dernières versions datées de la politique de sécurité », le DPO a répondu le 10 mars 2022 « En annexe 1, vous trouverez la politique de sécurité de l'information sur la base de laquelle les équipes et les Instances de la Clinique [redacted] travaillent. Celle-ci n'a pas évolué au fil du temps » (Pièce 11 du dossier administratif).

Le service d'inspection constate dans son rapport d'enquête technologique (pièce 13 du dossier administratif) que le document transmis date du 3 mars 2022, et qu'il s'agit de la première version du document.

Dans le rapport d'enquête (pièce 14 du dossier administratif), le service d'inspection relève, d'une part que, selon le DPO lui-même « la politique de sécurité de l'information de la Clinique (...) n'a pas évolué au fil du temps », et d'autre part, s'agissant du document du 3 mars 2022, qu'il aurait dû exister une version précédente du document.

Devant la Chambre contentieuse, la Requérante faisait valoir que le RGPD ne prévoit pas l'existence d'un seul document devant établir la « politique de sécurité de l'information », et qu'elle disposait bien, antérieurement au 10 mars 2022, d'une telle politique à travers différents documents, notamment règlement de travail du personnel de l'hôpital, [redacted] etc (cfr ses conclusions devant la Chambre contentieuse, pièce 21 du dossier administratif). Elle faisait valoir que la Chambre contentieuse ne devait pas se focaliser sur le seul document Politique de sécurité adopté le 10 mars 2022.

La Décision écarte la défense de la Requérante, aux motifs que « 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 » (Décision attaquée, § 78).

Par ces considérations, la Décision attaquée ne répond pas adéquatement à la défense avancée par la Requérante et introduit une exigence formelle qui n'est pas prévue par les dispositions du RGPD qu'elle applique.

La Décision attaquée justifie son exigence d'une politique formelle par les « normes minimales relatives à la sécurité de l'information et la vie privée pour les institutions de sécurité sociale en vertu de l'article 2, alinéa 1, 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 »). Cependant, comme le relève la Requérante, la compétence de la Chambre contentieuse est limitée à la vérification du respect du RGPD ; elle est sans compétence pour apprécier le respect d'autres obligations, en ce compris le respect des Normes minimales édictées sous l'égide de la Banque Carrefour de la Sécurité Sociale. Les Normes minimales ont par ailleurs la nature de lignes directrices, ou « soft law » et ne peuvent pas elles-mêmes fonder un constat de violation susceptible d'entraîner une sanction pécuniaire dont l'importance l'assimile à une peine.

La motivation de la Décision est par ailleurs entachée d'une contradiction en ce qu'elle considère, d'une part, que le document formel postérieur « Politique de sécurité » du 3 mars 2022 ne peut être pris en compte lors de l'examen de la violation du RGPD au jour de la cyberattaque, et, d'autre part, se prévaut de la déclaration faite dans ce document quant à un respect des Normes minimales pour considérer celles-ci applicables au jours de la cyberattaque.

Au vu de ce qui précède, le moyen est fondé en sa deuxième branche. La Décision est annulée s'agissant du constat de violation n° 2, pour défaut de motivation.

38. La troisième branche du moyen vise la Décision en ce qu'elle retient un constat n° 3 de violation, à savoir une violation des articles 5.1.f, 32 et 24 du RGPD pour défaut de prévoir « une politique et/ou une procédure de mise à jour de sécurité des équipements informatiques (logiciels) au moment de la violation des données » (Décision attaquée, § 96).

L'article 24 du RGPD dispose que :

« *1.Compte tenu de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques, le responsable du traitement met en oeuvre des mesures techniques et organisationnelles appropriées pour s'assurer et être en mesure de démontrer que le traitement est effectué conformément au présent règlement.* ***Ces mesures sont réexaminées et actualisées si nécessaire.***

2.Lorsque cela est proportionné au regard des activités de traitement, les mesures visées au paragraphe 1 comprennent la mise en oeuvre de politiques appropriées en matière de protection des données par le responsable du traitement.
3.L'application d'un code de conduite approuvé comme le prévoit l'article 40 ou de mécanismes de certification approuvés comme le prévoit l'article 42 peut servir d'élément pour démontrer le respect des obligations incombant au responsable du traitement » (mise en évidence par la Cour).

Le rapport d'enquête retient au titre de constatation n° 3 une « *inefficacité du choix de la politique et/ou procédure de mise à jour de sécurité des équipements informatiques (logiciels)* », ayant constaté que « *seuls les outils de sécurité sont contrôlés (…) le reste des logiciels n'est donc pas contrôlé en matière de sécurité* » ; le rapport retient que la vulnérabilité exploitée lors de l'incident [du 17 septembre 2021] (…) touchait les serveurs de messagerie Microsoft Exchange et fut rendue publique par le constructeur Microsoft le 13 juillet 2021. Cette vulnérabilité était catégorisée comme critique de par sa facilité d'exploitation, le fait qu'elle était exploitable sans privilège et à distance. Elle avait un score de base de 9.8. sur 10, ce qui aurait dû donner lieu, dans ce conteste, à des mesures de mitigation des risques » (p. 42 du rapport, pièce 14 du dossier administratif).

Se basant sur ce rapport, la Décision constate que la Requérante « *n'avait pas mis en place des mesures capables de l'alerter sur le fait que son traitement de données personnelles ne garantissait pas une sécurité appropriée aux risques* » et que celle-ci 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'un quelconque réexamination [sic] ou actualisation* » (§ 94 de la Décision).

La Chambre contentieuse en a déduit un manquement par la Requérante à son obligation de prévoir une politique et une procédure de mise à jour de sécurité des équipements informatiques (logiciels) et un manquement aux articles 5.1.f, 32 et 24 du RGPD.

La Requérante n'établit aucunement que, ce faisant, la Chambre contentieuse aurait commis une erreur manifeste d'appréciation. Elle se contente de réitérer devant la Cour ses arguments invoqués devant la Chambre contentieuse, consistant principalement à se prévaloir de mesures mises en place après l'incident. En aucune façon elle n'établit que la Décision attaquée, adéquatement motivée, procéderait d'une erreur manifeste d'appréciation.

La violation aux articles 24 et 32 du RGPD est établie. La référence à l'article 5.1.f) est dépourvue de contenu autonome et n'ajoute rien au constat de violation ; il s'agit de la référence au principe général de sécurité.

39. La quatrième branche du moyen vise la Décision en ce qu'elle retient, au titre du constat n° 4 de violation « Autres mesures de sécurité », un défaut de prévoir « un véritable programme de

formation et de sensibilisation des employés au RGPD » (Décision attaquée, § 105 ; violation des articles 5.1.f, 32 et 24 du RGPD).

Le rapport d'enquête retient au titre de constatation n° 4 que la Requérante n'établit pas avoir implémenté une campagne de sensibilisation à la sécurité de l'information au sein de son personnel ; elle n'a fait que réagir à chaud à chaque incident : séances de formation et de sensibilisation au hameçonnage après l'incident de 2019 et ensuite suite à la nouvelle cyberattaque. Ceci alors que « la sensibilisation à la sécurité de l'information est un point essentiel (5.4.) des Normes minimales (…) » (p. 43 du rapport, pièce 14 du dossier administratif).

Selon la Décision, « *les employés d'un hôpital en contact avec des catégories spéciales de données personnelles doivent recevoir une formation appropriée et régulière relative aux normes minimales à respecter dans le cadre du traitement de telles données, en fonction de la pertinence pour leur rôle ou fonction. 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 (…)* » (§ 99 et 100 de la Décision).

A raison, la Requérante fait valoir que l'infraction retenue de défaut de programme de formation et de sensibilisation des employés au RGPD ne repose sur aucune exigence légale précise. Les articles du RGPD invoqués (5.1.f, 32 et 24) ne contiennent pas en eux-mêmes une obligation précise de formation et de sensibilisation des employés au RGPD. La Norme Minimale 5.4. prévoit une telle obligation d'organiser « *au moins une fois par an (…) une campagne de sensibilisation ou une session d'information relative à la sécurité de l'information et à la vie privée (…)* » mais l'APD n'est pas chargée du respect de ces Normes Minimales, qui ne constituent que des lignes directrices qui ne peuvent fonder un constat de violation susceptible de justifier une peine (cfr supra).

Le moyen est fondé en sa quatrième branche. La Décision est annulée en ce qui concerne le constat de violation n° 4 pour ce qui concerne le défaut de programme de formation et de sensibilisation des employés au RGPD.

40. La cinquième branche du moyen vise la Décision en ce qu'elle retient, au titre du constat n° 4 de violation « Autres mesures de sécurité », la non mise 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* » (Décision attaquée, § 113 ; violation des articles 5.1.f, 32 et 24 du RGPD).

Selon la Décision, « *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) (…) inclut également la capacité à préserver des logs en vue d'analyses ultérieures lors de violations de données* » (§ 107 de la Décision).

Le rapport d'enquête a aussi retenu un grief spécifique en rapport avec une absence de préservation des logs (p. 60 du rapport, pièce 14 du dossier administratif).

Comme l'invoque le moyen, la Chambre contentieuse ajoute cependant, ce faisant, à l'article 32 du RGPD une obligation particulière qui n'y figure pas, à savoir une obligation de préserver les logs en vue d'une analyse *a posteriori* des actions de piratage. L'obligation qu'elle ajoute paraît de surcroit constituer, dans son appréciation, une obligation de résultat.

Se contentant de cette affirmation erronée, la Décision n'établit pas en quoi, en l'espèce, une obligation de prévoir un système de préservation des logs aurait fait partie des mesures techniques et organisationnelles appropriées au sens de l'article 32.1. du RGPD.

La Décision n'est donc pas régulièrement et adéquatement motivée en ce qu'elle retient une violation des articles 5.1.f, 32 et 24 en rapport avec une absence de mesure de préservation des logs.

La préservation des logs afin de pouvoir analyser les intrusions participe incontestablement d'une bonne politique de sécurité et c'est à juste titre qu'il y est fait référence[10] dans les Lignes directrices 01/2021 de l'EDPB « Exemples concernant la notification de violations de données à caractère personnel » adoptées le 14 décembre 2021, ainsi que dans les Normes minimales (point 5.9.5.). Cela étant, ceci n'implique pas que cette mesure doive être considérée comme prévue par l'article 32 du RGPD lui-même et que son non-respect expose son auteur à une peine.

Le moyen est fondé en sa cinquième branche. La Décision est annulée en ce qui concerne le constat de violation n° 4 pour ce qui concerne la non-préservation des logs.

41. La sixième branche du moyen vise la Décision en ce qu'elle retient, au titre du constat n° 4 de violation « Autres mesures de sécurité », un défaut de « mise en place des audits réguliers et systématiques pour tester, analyser et évaluer l'efficacité des mesures techniques et organisationnelles (...) et assurer la sécurité des traitements de données » (Décision attaquée, § 119 ; violation des articles 5.1.f, 32 et 24 du RGPD).

La Décision invoque l'article 32.1.d) du RPGD, qui prévoit, parmi les mesures techniques et organisationnelles appropriées à mettre en place afin de garantir un niveau de sécurité adapté au risque, entre autres, 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 ».

[10] Pas de manière très explicite cependant.

Elle se réfère aussi aux Normes minimales prévoyant que toute institution de sécurité sociale « 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 » (§ 117 de la Décision).

Elle retient un manquement aux articles 5.1.f), 32 et 24 du RGPD au motif que la Requérante n'avait pas mis en place des audits réguliers et systématiques pour tester, analyser et évaluer l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement des données.

Elle retient qu'aucun audit n'avait été réalisé avant l'incident du 21 septembre 2021, tandis que plusieurs ont été réalisés ultérieurement.

Le rapport d'enquête a aussi souligné l'absence de recours à des audits systématiques de la qualité de la sécurité des données à caractère personnel (p. 61 du rapport, pièce 14 du dossier administratif).

Même si la Chambre contentieuse ne pouvait fonder un constat de violation du RGPD sur les Normes minimales, pour les motifs indiqués précédemment, il n'en demeure pas moins que, comme elle l'indique, la mise en place d'audits réguliers est prévue par le texte même de l'article 32.1.d) du RGPD.

La Requérante n'établit pas qu'en retenant pour ce motif une violation de l'article 32 du RGPD, la Décision ne serait pas adéquatement motivée ou procéderait d'une erreur manifeste d'appréciation.

Il n'y a pas non plus de défaut de motivation de la Décision, l'application de l'article 32 du RGPD ne requérant pas que soit à chaque fois explicité l'appréciation de « l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques », et la hauteur des risques en matières de données de santé justifiant les audits périodiques, indépendamment des ressources de l'hôpital.

Le moyen n'est pas fondé en cette branche.

42. La septième branche du moyen vise la Décision en ce qu'elle retient, au titre du constat n° 4 de violation « Autres mesures de sécurité », un défaut de « robustesse du mot de passe au niveau de sécurité requis pour protéger l'accès à des dossiers informatisés de patients » (Décision attaquée, § 126 ; violation des articles 5.1.f, 32 et 24 du RGPD).

Le rapport d'enquête constate sur la base du « formulaire de demande de connexion utilisateur au dossier informatisé du patient » que ce formulaire prévoit que « le mot de passe doit faire entre 6 et 8 positions. Il ne peut pas être une répétition du nom, prénom, service ou initiales de l'utilisateur » et

estime que « l'exigence d'un mot de passe de si faible qualité n'est pas à même d'assurer une sécurisation suffisante de l'accès aux données du dossier informatisé du patient » (p. 63 du rapport).

La Décision retient que « dans un contexte hospitalier où la protection des données de santé des patients est cruciale, un mot de passe très robuste est nécessaire » et énonce que 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, prévoit que « Un mot de passe suffisamment long compte minimum 12 caractères » » (§ 122 de la Décision).

La Requérante fait valoir que la « Note de sécurité… » sur laquelle la Décision se fonde et selon laquelle « un mot de passe suffisamment long compte minimum 12 caractères » n'était pas mentionnée dans le rapport d'enquête et qu'elle n'a pas été invitée à s'expliquer sur ce document.

Si c'est exact, il n'apparaît cependant pas que cette violation a eu un impact sur la Décision, dès lors qu'à tout le moins devant la Cour, le droit à la contradiction de la Requérante est respecté.

Or, précisément, alors qu'elle a l'occasion de critiquer la référence contenue dans la Décision, la Requérante n'expose en rien en quoi une exigence de 12 caractères serait critiquable pour assurer la robustesse d'un mot de passe pour accéder à des données de santé, et en quoi la Décision procéderait d'une mauvaise application du RGPD ou en quoi la Chambre contentieuse aurait commis une erreur manifeste d'appréciation en considérant qu'exiger un mot de passe de 6 à 8 caractères n'assurerait pas la robustesse nécessaire à un tel mot de passe.

Il n'y a pas non plus de défaut de motivation de la Décision, l'application de l'article 32 du RGPD ne requérant pas que soit à chaque fois explicité l'appréciation de « l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques », et l'exigence d'un mot de passe suffisamment robuste n'étant au demeurant en rien coûteuse.

Le moyen n'est donc pas fondé en cette branche.

HUITIEME MOYEN REQUERANTE : moyen pris de la violation du principe du raisonnable et de proportionnalité et des articles 2 et 3 de la loi du 29 juillet 1991 relative à la motivation formelle des actes administratifs : la Chambre contentieuse ne respecte pas le principe de motivation lorsqu'elle ne tient pas compte des moyens à la disposition de l'Hôpital lorsqu'elle évalue les mesures de sécurité implémentées par l'Hôpital.

Ce moyen critique les §§ 60 à 126 de la Décision attaquée

Huitième moyen APD.

Résumé des positions des parties

43. La **Requérante** fait valoir que la Chambre contentieuse ne tient pas suffisamment compte des moyens limités de l'Hôpital lorsqu'elle évalue les mesures de sécurités implémentées par celui-ci. Lorsqu'il s'agit d'assurer la sécurité des données, le RGPD n'impose qu'une obligation de moyens : prendre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté aux risques, mais en tenant compte des coûts de mise en œuvre.

La problématique des difficultés de financement des hôpitaux est de notoriété publique et ce n'est qu'en juillet 2022 que la Requérante a bénéficié d'une enveloppe de l'ordre de 100.000 EUR (somme très inférieure aux investissements déjà consentis en matière de cybersécurité). Afin de pouvoir considérer que la Requérante aurait violé les articles 5, point 2, 24 ou 32 du RGPD (quod non), la Chambre contentieuse aurait dû motiver en quoi la Requérante aurait pu consacrer encore davantage de budget à la cybersécurité qu'elle ne l'a fait, *a fortiori* dans un contexte de crise sanitaire (Covid-19). À aucun moment, la Décision attaquée ne prend en considération les moyens financiers que la Requérante a déjà dû dégager, en les mettant en rapport avec ses ressources disponibles, ce qui viole les principes du raisonnable et de proportionnalité. En toute hypothèse, la Décision attaquée n'est donc pas dûment motivée.

44. L'**APD** fait valoir que la Chambre contentieuse a bien appliqué le principe de proportionnalité en mettant en balance les intérêts en présence. Ce faisant, la Chambre contentieuse a réévalué le montant de l'amende de 390.000,00 EUR à 200.000,00 EUR et la motivation permet de comprendre les motifs de la décision. La Chambre contentieuse a donc tenu compte des capacités financières et des contraintes budgétaires auxquelles la requérante était soumise lors de l'établissement du

montant de l'amende et la Requérante ne démontre pas que la décision présenterait un défaut de proportionnalité manifeste. En tout état de cause, les efforts budgétaires consentis après les attaques auraient pu être évités si cette dernière avait adopté les mesures nécessaires pour respecter les exigences du RGPD.

Discussion et décision par la Cour

45. Comme l'indique la Requérante, le moyen vise les §§ 60 à 126 de la Décision attaquée, soit les constats de manquements n° 1 à 4 retenus à charge de la Requérante, et non les passages relatifs à la sanction. L'application des principes évoqués au moyen concernant les passages relatifs à la sanction feront l'objet d'un examen ultérieur.

Contrairement à ce que sous-tend le moyen, l'application de l'article 32 du RGPD ne requiert pas que soit à chaque fois explicité l'appréciation de « l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques ».

La Requérante n'établit ni défaut de motivation, ni violation des principes de bonne administration, en particulier du principe de proportionnalité et du raisonnable.

La critique reprise à ce moyen a par ailleurs déjà fait l'objet d'une réponse dans le cadre du moyen précédent où elle était déjà développée et la cour renvoie à celle-ci.

Le moyen n'est pas fondé.

NEUVIEME MOYEN REQUERANTE : La Chambre contentieuse outrepasse ses compétences lorsqu'elle constate que l'Hôpital aurait manqué au respect 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 (BCSS).
Neuvième moyen APD.

Ce moyen critique les §§ 73 à 75 de la Décision attaquée.

Résumé des parties

46. La **Requérante** allègue que la Chambre contentieuse n'a pas de compétence en matière de contrôle du respect des Normes minimales imposées par la Banque Carrefour de la Sécurité sociale. Elle ne peut pas s'octroyer des compétences supplémentaires consistant à contrôler et sanctionner le

respect de normes alors que la loi ne lui attribue pas cette tâche ou que la loi l'attribue explicitement à une autre instance, en faisant rentrer ces normes dans 'l'état de connaissance' dont il est question à l'article 32 du RGPD. En agissant de la sorte, elle outrepasse manifestement ses compétences.

47. L'**APD** soutient que la prise en compte des Normes minimales est parfaitement justifiée à partir du moment où l'article 32, point 1, du RGPD fait référence à la prise en compte de 'l'état des connaissances'. La Chambre contentieuse ne se prononce pas sur le non-respect des Normes minimales en tant que tel. Elle tient compte des Normes minimales uniquement dans le cadre de l'appréciation de l'état des connaissances et ceci est indispensable pour évaluer si la Requérante a mis en place les mesures techniques et organisationnelles démontrant qu'elle dispose d'une politique de sécurité de l'information formelle et actualisée. La Chambre contentieuse n'a donc pas outrepassé ses compétences.

Discussion et décision par la Cour

48. Selon la Requérante, ce moyen vise la Décision attaquée en ses §§ 73 à 75, concernant le constat de violation n° 2.

Dès lors que, par l'accueil partiel du septième moyen, en sa deuxième branche, la Décision est annulée concernant ce constat, il n'est pas nécessaire d'avoir égard à ce moyen, qui ne saurait entraîner une annulation plus étendue.

V.2.3. MOYENS RELATIFS A LA SANCTION

DIXIEME MOYEN REQUERANTE : moyen pris de la violation de l'articles 83.7 du RGPD lu en combinaison avec l'article 221, §2 de la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel : les autorités publiques ne peuvent pas faire l'objet d'une amende administrative.
Dixième moyen APD.

Ce moyen critique les §§ 127 à 146 de la Décision attaquée.

Résumé des parties

49. La **Requérante** soulève qu'elle remplit les conditions de l'art. 5, al. 2, 3° de la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, et doit donc être considéré comme une « autorité publique » pour l'application

de cette loi, ce qui conduit à ce qu'une amende ne puisse pas lui être imposée, par application de l'article 221, § 2 de la même loi. La Décision attaquée repose sur une erreur manifeste d'appréciation ; la condition d'être 'financée majoritairement par les autorités publiques ou organismes mentionnés au 1° et 2'', telle que prévue à l'article 5 de la loi est remplie.

La Requérante peut se prévaloir de l'exception prévue par l'article 221, §2, de la loi du 30 juillet 2018, s'agissant de l'imposition d'une amende administrative sur la base de l'article 83 du RGPD.

La Décision attaquée viole l'article 221, §2, de la loi du 30 juillet 2018 et doit être annulée.

50. L'**APD** conclu que la Requérante ne remplit pas les conditions requises pour être considérée comme une autorité publique au sens de l'article 5, 3° de la loi du 30 juillet 2018 et la Chambre contentieuse à cet égard a répondu à tous les arguments dans la Décision attaquée. La Requérante n'avance aucun nouvel argument.

Discussion et décision par la Cour

51. L'article 5, al. 2 de la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel dispose 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'État 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° ».

L'article 221 § 2 de la même loi 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 ».

Par la combinaison de ces deux dispositions, les « autorités publiques » telles que définies par le loi ne peuvent se voir infliger une amende administrative telle que prévue par l'article 83 du RGPD, sauf si elles offrent des biens ou des services sur un marché.

52. La Requérante reproche à la Décision attaquée de ne pas avoir accepté de la considérer comme « autorité publique » au sens de l'article 5, al. 2, 3° de la loi du 30 juillet 2018, et soutient qu'elle remplit les conditions prévues à cette disposition.

L'article 5, alinéa 2 de la loi du 30 juillet 2018 comprend une définition de l' « autorité publique » inspirée de celle d' « instance publique » figurant à l'article 2 de loi du 4 mai 2016 relative aux données ouvertes et à la réutilisation des informations du secteur public[11] ; c'est ce qui ressort de l'Exposé des motifs de la loi[12], sans que le législateur ne se soit expliqué sur la pertinence de cet emprunt.

Il résulte par contre des débats parlementaires qu'alors que le Conseil d'Etat s'était inquiété de la non-application des amendes administratives aux autorités publiques, y voyant un risque de discrimination par rapport aux responsables du traitement du secteur privé, et donc un risque de non-respect des articles 10 et 11 de la Constitution.[13] Pour contrer ce risque, différents amendements ont été déposés, et l'amendement n° 44 de [redacted] a été adopté, à savoir l'ajout, à l'article 221 en projet, des mots « sauf s'il s'agit de personnes morales de droit public qui offrent des biens ou des services sur un marché »[14], de manière à créer « un terrain plus égal entre les autorités publiques et le marché privé ».[15]

A la lumière de ce qui précède, il apparaît qu'il y a lieu d'interpréter strictement la notion d' « autorité publique », l'intention du législateur n'ayant pas été d'attraire des opérateurs privés sous ce vocable. De même, il convient de tenir compte que l'exemption pour les autorités publiques découle d'une latitude laissée aux Etats membres à l'article 83.7. du RGPD pour « les autorités publiques et organismes publics » établis sur leur territoire, ce qui justifie aussi de ne pas englober dans le vocable « autorités publiques » des opérateurs privés.

Ainsi, il apparait que la Requérante, constituée sous la forme d'une ASBL, ne constitue pas une « autorité publique » au sens de la loi du 30 juillet 2018. Si, naturellement, il s'agit d'une entité dotée de la personnalité juridique, elle ne peut être considérée comme « ayant *été créées pour satisfaire spécifiquement des besoins d'intérêt général ayant un caractère autre qu'industriel ou commercial* ».

---

[11] Loi assurant elle-même la transposition de la Directive (UE) 2019/1024 du 20 juin 2019 du Parlement européen et du Conseil concernant les données ouvertes et la réutilisation des informations du secteur public (cfr la définition des « organismes de droit public » qui figure à l'article 2 de ladite Directive).
[12] Doc. Parl., Chambre, Doc. 54, 3126/001, p. 17.
[13] Avis du conseil d'Etat, p. 46 à 48.
[14] Doc. Parl, Chambre, Doc. 54, 3126/002, p. 55.
[15] Ibidem.

La notion de besoins d'intérêt général doit s'entendre au sens strict, comme un besoin lié à l'exercice d'une certaine autorité, et ne peut être confondue avec le but désintéressé poursuivi notamment par toute ASBL.

Par ailleurs, comme l'expose la Décision, si l'objet social de la Requérante est d'améliorer la santé des habitants (de Liège), comme elle le soutient, elle poursuit également un but économique, de sorte qu'elle ne peut en tout état de cause être considérée comme ayant été créée pour satisfaire spécifiquement des besoins d'intérêt général ayant un caractère autre qu'industriel ou commercial.

En effet elle poursuit des activités hospitalières c'est -à-dire qu'elle traite – contre paiement - des patients aussi bien de jour que de nuit pour des soins médicaux spécialisés (rapport cité par la Requérante p 74 de ses conclusions).

La condition liée à la création spécifique pour satisfaire des besoins d'intérêt général ayant un caractère autre qu'industriel ou commercial, il n'est pas nécessaire d'examiner celle relative à son financement.

A titre surabondant, à supposer même qu'il faudrait considérer que les conditions de l'article 5, 3° seraient réunies dans son chef, il conviendrait alors de faire échec à l'exclusion du champs d'application des amendes, dès lors que la Requérante offre des biens et des services sur un marché.

Il résulte en effet clairement des travaux parlementaires que l'intention du législateur, pour éviter le risque de discrimination relevé par le Conseil d'Etat dans son avis, était que, lorsqu'un service peut être opéré tant par une autorité publique que par un opérateur privé, comme dans le cas d'un hôpital, les responsables de traitement ne soient pas dispensés de la possibilité d'être sanctionnés par une amende.

En décidant que la Requérante ne pouvait pas bénéficier de l'exclusion prévue à l'article 221, § 2 de la loi du 30 juillet 2018, la Décision n'a dès lors pas violé les dispositions visées au moyen.

Le moyen est non fondé.

Moyens 11 à 13

53. La Cour examinera ensemble les moyens 11 à 13 de la requérante, relatifs au principe de l'amende infligée et à son *quantum*.

ONZIEME MOYEN REQUERANTE : moyen pris de la violation de l'article 83.2. du RGPD : la Chambre contentieuse de l'APD ne tient pas compte de l'ensemble des critères énumérés à l'article 83.2. du RGPD pour définir la sanction appropriée et le montant de l'amende.

Onzième moyen APD.

Ce moyen critique les §§ 147 à 191 de la Décision attaquée.

Résumé du moyen

54. Selon la **Requérante**, bien que la Chambre contentieuse dispose d'un pouvoir discrétionnaire pour décider d'imposer une amende administrative et pour fixer le montant de cette amende, l'exercice de ce pouvoir doit toutefois respecter les limites imposées par le RGPD et est soumis au contrôle de la Cour. *En l'espèce*, l'APD n'a pas procédé à l'examen détaillé de tous les critères prévus par le RGPD) avant de décider d'infliger une amende et d'en calculer le montant.

Premièrement, la Chambre contentieuse estime que l'infraction commise par la Requérante atteint un niveau de gravité moyen sur la base de constats erronés. Les traitements ayant fait l'objet de l'examen de la Chambre Contentieuse concernent la gestion des systèmes informatiques de la Requérante (messagerie électronique du personnel) et les violations constatées ne concernent donc pas l'activité principale du responsable du traitement. En tout cas, la Requérante a mis en place les mesures techniques appropriées aux risques et même plus encore. En tout état de cause, le niveau de gravité du manquement est faible.

Deuxièmement, la Chambre contentieuse, à tort, tient compte du fait que la Requérante traite les données de 300.000 patients. Or, ce sont uniquement les données du serveur de messagerie électronique du personnel qui ont été touchées par la cyberattaque et la violation de données. Au final, seuls les soins dispensés pendant trois jours ont très légèrement été perturbés, car il a fallu fonctionner en mode papier. Au maximum 500 patients étaient traités durant la période concernée.

Troisièmement, la Chambre contentieuse estime à tort que les mesures techniques et organisationnelles de la Requérante n'ont été prises qu'après la seconde violation de données, à savoir trois ans et quatre mois après l'entrée en vigueur du RGPD. La Requérante a pris des mesures de sécurité adaptées et les a améliorées de façon continue. Par ailleurs, la Décision attaquée ne pouvait pas retenir comme date de début de l'infraction avril 2019 en se basant sur la date de survenance de la première cyberattaque, au sujet de laquelle aucun document ne figure dans le dossier du Service d'inspection. En outre, la Décision attaquée ne détermine pas avec précision le comportement infractionnel qu'elle estime, au surplus des mesures correctrices prescrites, devoir sanctionner par l'application d'une amende de 200.000,00 €. Ces manques de motivation doivent être sanctionnés par l'annulation de la Décision attaquée.

Quatrièmement, la Requérante a démontré avec suffisance que le dommage subi en raison de l'attaque était négligeable et qu'aucune donnée n'a été volée lors de l'incident. Cet élément constitue une circonstance atténuante que la Décision aurait dû prendre en considération ; ne l'ayant pas fait, elle est entachée d'une erreur manifeste d'appréciation et n'est pas dûment motivée sur ce

point. En outre, et cinquièmement, en estimant que l'activité de base de la Requérante implique le traitement de données sensibles ce qui justifie que la négligence commise par la Requérante soit jugée sérieuse, la Chambre contentieuse commet une erreur manifeste d'appréciation.
Au regard de l'importance des mesures de sécurité mises en place par la Requérante par rapport aux moyens financiers disponibles, il ne peut pas être considéré qu'elle a été négligente.

Sixièmement, en omettant de prendre en compte le degré de responsabilité du responsable du traitement ou du sous-traitant, compte tenu des mesures techniques et organisationnelles qu'ils ont mises en œuvre en vertu des articles 25 et 32 du RGPD, la Chambre contentieuse manque à son obligation de motivation.

Septièmement, la Chambre contentieuse ne tient pas suffisamment compte des nombreux moyens mis en œuvre par la Requérante pour remédier à la violation alors que son comportement devrait constituer une circonstance atténuante. Par ailleurs et huitièmement, en ne tenant pas compte du degré de coopération établi avec l'APD (circonstance atténuante), la Chambre contentieuse a commis une erreur manifeste d'appréciation.

Neuvièmement, les données de santé n'ont pas été compromises lors de l'attaque. Ce critère donc aurait dû être considéré comme neutre et ne pouvait être retenu deux fois contre la Requérante (pour définir le niveau de gravité et comme circonstance aggravante). De surcroît, dixièmement, la Chambre contentieuse a commis une erreur manifeste d'appréciation et n'a pas correctement motivé sa décision en ne tenant pas compte de l'absence de code de conduite au titre de circonstance atténuante.

Onzièmement, la Décision attaquée ne pouvait tenir compte du précédent de 2019, puisque cet incident n'avait fait l'objet d'aucune décision antérieure. Des faits ne peuvent pas être considérés comme un précédent si l'APD n'avait à l'époque pas estimé nécessaire de les poursuivre. La Chambre contentieuse aurait dû retenir les éléments suivants comme circonstances atténuantes : (i) l'absence d'une plainte, ce qui concorde avec l'absence de violation de la confidentialité des données et de tout dommage physique ou autre, (ii) le fait que les hôpitaux sont des cibles privilégiées pour les attaques informatiques, (iii) la crise Covid-19 et (iv) les investissements réalisés pour améliorer les mesures de sécurité, en ce compris les mesures mises en place après l'attaque.

55. L'**APD** conteste le moyen en toutes ses branches.

DOUZIEME MOYEN REQUERANTE : moyen pris de la violation de l'article 83.1. du RGPD, lu en combinaison avec le principe de minutie, du principe du raisonnable et de proportionnalité : l'amende administrative imposée à l'Hôpital ne respecte pas les exigences d'effectivité, de proportionnalité et de dissuasion.
Douzième moyen APD.

Résumé du moyen

56. Premièrement, la **Requérante** fait valoir que l'amende administrative n'est pas une sanction effective. La Requérante n'a pas eu de comportement négligent et n'a pas commis de manquement grave au RGPD. Une sanction moins sévère, telle qu'une réprimande, est efficace en elle-même, dès lors que la situation sanctionnée n'est plus la situation actuelle lors de la prise de Décision, qui constate que les manquements sanctionnés ont pris fin. L'ajout d'une amende administrative à l'ordre de mise en conformité n'atteint pas les objectifs pour lesquels elle peut être imposée, mais va bien au-delà. La Chambre contentieuse confond les exigences d'effectivité et de dissuasion de l'amende, ce qui entache donc la motivation de sa décision.

Deuxièmement, considérer la sanction à l'égard d'un hôpital en grande difficulté, comme 'un exemple' pour les autres hôpitaux dont la plupart sont des autorités publiques qui ne peuvent pas se voir infliger d'amende administrative, est contraire aux principes généraux qui appellent à un procès équitable (article 6 CEDH). En outre, la Chambre contentieuse ne traite pas la Requérante de la même manière que tout hôpital belge ayant subi une cyberattaque et se trouvant dans une situation comparable mais qui a eu 'la chance' de ne pas être le premier hôpital à faire l'objet d'une procédure au fond devant la Chambre contentieuse de l'APD. Ainsi, elle viole le principe de non-discrimination. En voulant 'envoyer un message fort', la Chambre contentieuse sanctionne de manière disproportionnée la Requérante. La sanction n'est donc pas dissuasive.

Troisièmement, vue que les manquements constatés par l'APD ne représentent pas un niveau moyen de gravité et que des circonstances atténuantes n'ont pas été prises en compte, les sanctions définies sans tenir compte de ces éléments sont disproportionnées. En outre, l'amende administrative imposée n'est pas proportionnée au regard de la capacité financière de la Requérante et met tout simplement irrémédiablement en danger sa santé financière. Finalement, c'est le chiffre d'affaires de l'exercice précédent l'incident (2020) qui aurait dû être pris en considération.

En conclusion, la Décision attaquée n'est pas dûment motivée et l'amende administrative est disproportionnée. Si le principe d'une sanction est maintenu, la sanction prononcée soit celle de la réprimande. A titre subsidiaire, la Requérante sollicite que le montant de l'amende administrative soit réduit à 1 euro symbolique. A titre infiniment subsidiaire, les violations de l'article 5 du RGPD

n'étant pas dûment établies, seul le plafond de l'amende prévu à l'article 83, point 4, peut être pris comme point de départ du calcul de l'amende, de sorte qu'elle doit au minimum être réduite de 50%.

57. L'**APD** conteste le moyen en toutes ses branches.

TREIZIEME MOYEN REQUERANTE : moyen pris de la violation des principes de bonne administration : la Chambre contentieuse de l'APD ne respecte pas le principe de motivation lorsqu'elle ne tient pas compte des arguments soulevés par l'Hôpital dans sa réponse au formulaire de sanction

Treizième moyen APD.

Résumé des parties

58. Par son treizième moyen, la **Requérante** soulève que la Chambre contentieuse ne tient pas compte des arguments soulevés dans la réponse au formulaire de sanction. Tout particulièrement, la Décision attaquée ne tient compte de la charge financière que représentent les investissements déjà consentis, tant avant qu'après la seconde attaque. En plus, la Décision attaquée confondrait chiffres d'affaires et résultat lorsqu'elle évalue la capacité économique de la Requérante. En agissant de la sorte, la Chambre contentieuse manque à son obligation de motivation. Si le principe d'une sanction est maintenu par la Cour, la sanction prononcée soit celle de la réprimande et, à titre subsidiaire, le montant de l'amende administrative doit être réduit à 1 euro symbolique.

59. L'**APD** soulève que la Chambre contentieuse a - au moins indirectement - tenu compte des dépenses en sécurité de la Requérante, puisqu'elle a tenu compte des mesures implémentées pour atténuer le dommage au titre de circonstance atténuante. En l'espèce, la Chambre contentieuse s'est tenue au chiffre d'affaires de la Requérante pour fixer le montant de départ de l'amende administrative pour lequel elle se doit d'appliquer le mode de calcul des amendes administratives prévu par le RGPD et ne peut s'en écarter. La capacité financière de la Requérante a été prise en considération et a été considéré comme une circonstance atténuante.

Discussion et décision par la Cour quant aux moyens 11, 12 et 13

60. L'article 83 du RGPD se lit comme suit (mises en évidence ajoutées):

« Article 83 Conditions générales pour imposer des amendes administratives

1.Chaque autorité de contrôle veille à ce que les amendes administratives imposées en vertu du présent article pour des violations du présent règlement visées aux paragraphes 4, 5 et 6 soient, dans chaque cas, ***effectives, proportionnées et dissuasives****.*

2.Selon les caractéristiques propres à chaque cas, les amendes administratives sont imposées en complément ou à la place des mesures visées à l'article 58, paragraphe 2, points a) à h), et j).

Pour décider s'il y a lieu d'imposer une amende administrative et pour décider du montant de l'amende administrative, ***il est dûment tenu compte, dans chaque cas d'espèce, des éléments suivants****:*

a) 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;*

b) le fait que la violation a été commise ***délibérément ou par négligence****;*

c) toute ***mesure prise*** *par le responsable du traitement ou le sous-traitant pour* ***atténuer le dommage*** *subi par les personnes concernées;*

d) le degré de responsabilité du responsable du traitement ou du sous-traitant, compte tenu des mesures techniques et organisationnelles qu'ils ont mises en oeuvre en vertu des articles 25 et 32;

e) toute ***violation pertinente commise précédemment*** *par le responsable du traitement ou le sous-traitant;*

f) le ***degré de coopération*** *établi avec l'autorité de contrôle en vue de remédier à la violation et d'en atténuer les éventuels effets négatifs;*

g) les ***catégories de données*** *à caractère personnel concernées par la violation;*

h) la ***manière dont l'autorité de contrôle a eu connaissance de la violation****, notamment si, et dans quelle mesure, le responsable du traitement ou le sous-traitant a notifié la violation;*

i) lorsque des mesures visées à l'article 58, paragraphe 2, ont été précédemment ordonnées à l'encontre du responsable du traitement ou du sous-traitant concerné pour le même objet, le respect de ces mesures;

j) ***l'application de codes de conduite*** *approuvés en application de l'article 40 ou de mécanismes de certification approuvés en application de l'article 42; et*

k) ***toute autre circonstance aggravante ou atténuante applicable aux circonstances de l'espèce****, telle que les avantages financiers obtenus ou les pertes évitées, directement ou indirectement, du fait de la violation.*

3.Si un responsable du traitement ou un sous-traitant viole délibérément ou par négligence plusieurs dispositions du présent règlement, dans le cadre de la même opération de traitement ou d'opérations de traitement liées, le montant total de l'amende administrative ne peut pas excéder le montant fixé pour la violation la plus grave.

4.Les violations des dispositions suivantes font l'objet, conformément au paragraphe 2, d'amendes administratives pouvant s'élever ***jusqu'à 10 000 000 EUR ou, dans le cas d'une entreprise, jusqu'à 2 % du chiffre d'affaires annuel*** *mondial total de l'exercice précédent, le montant le plus élevé étant retenu:*

a) les obligations incombant au responsable du traitement et au sous-traitant en vertu des articles 8, 11, 25 à 39, 42 et 43;

b) les obligations incombant à l'organisme de certification en vertu des articles 42 et 43;
c) les obligations incombant à l'organisme chargé du suivi des codes de conduite en vertu de l'article 41, paragraphe 4.

5. Les violations des dispositions suivantes font l'objet, conformément au paragraphe 2, d'amendes administratives pouvant s'élever ***jusqu'à 20 000 000 EUR ou, dans le cas d'une entreprise, jusqu'à 4 % du chiffre d'affaires annuel*** *mondial total de l'exercice précédent, le montant le plus élevé étant retenu:*
a) les principes de base d'un traitement, y compris les conditions applicables au consentement en vertu des articles 5, 6, 7 et 9;
b) les droits dont bénéficient les personnes concernées en vertu des articles 12 à 22.
(...)

8.L'exercice, par l'autorité de contrôle, des pouvoirs que lui confère le présent article est soumis à des garanties procédurales appropriées conformément au droit de l'Union et au droit des États membres, y compris un recours juridictionnel effectif et une procédure régulière.
(...) ».

Par ailleurs, l'article 100 de la Loi APD énumère les sanctions que la Chambre contentieuse a le pouvoir de prononcer (cfr énumération de 1° à 16 °). La faculté d'infliger une amende administrative n'est que la treizième sanction dans l'énumération légale.

L'économie générale du RGPD indique que le législateur a voulu offrir à l'autorité nationale un panel de sanctions à appliquer en fonction de chaque cas d'espèce, dont l'imposition d'amendes administratives en application de l'article 83 de ce règlement, « en complément ou à la place » des autres mesures correctrices énumérées à cet article 58, paragraphe 2 (avertissements, rappels à l'ordre, injonctions).

Le considérant 148 du RGPD énonce notamment qu'il est permis aux autorités de contrôle, lorsqu'il s'agit d'une violation mineure ou si l'amende administrative susceptible d'être imposée constitue une charge disproportionnée pour une personne physique, de s'abstenir d'imposer une amende administrative et, à sa place, de prononcer un rappel à l'ordre.

Le but fondamental de la législation, tant européenne que belge, n'est en effet pas de sanctionner en infligeant des amendes pour le moindre manquement aux prescrits légaux. L'objectif est d'assurer l'effectivité du droit et la protection des données.

Il appartient à la Chambre contentieuse de justifier sa décision d'infliger une amende administrative au vu des dispositions qui précèdent et au vu de l'appréciation concrète des circonstances de la cause.

61. La Décision attaquée retient les violations suivantes au RGPD :

- 1°) Violation de l'article 35.3. du RGPD - manquement à l'obligation de réaliser une AIPD ;
- 2°) Violation des articles 5.1.f et 32 du RGPD – manquement à l'obligation d'établir une politique de sécurité de l'information formelle ;
- 3°) Violation des articles 5.1.f), 32 et 24 du RGPD – manquement à l'obligation de prévoir une politique et une procédure de mise à jour de sécurité des équipements informatiques (logiciels) ;
- 4°) Violation des articles 5.1.f), 32 et 24 du RGPD du fait de manquements à d'autres mesures de sécurité :
    - Absence d'un véritable programme de formation et sensibilisation des employés au RGPD ;
    - Absence de mise en place de mesures adéquates de préservation des logs contre des suppressions malveillantes ou le chiffrement ;
    - Absence de mise en place d'audits réguliers et systématiques ;
    - Non-robustesse des mots de passe pour protéger l'accès aux dossiers informatisés de patients.

Elle impose sur cette base des ordres de mise en conformité (cfr infra, examen du moyen 14) ainsi qu'une amende administrative de 200.000 € pour les violations des articles 35.3, 32, 5.1.f et 24 du RGPD.

Il résulte de l'examen du septième moyen que la Décision est partiellement annulée ; elle est annulée en ce qui concerne :

- le constat de violation 2°) ;
- le constat de violation 4°) en ce qui concerne les deux premiers éléments retenus (absence de programme de formation et absence de préservation des logs).

La violation de l'article 35.3 du RGPD demeure, ainsi que celle des articles 5.1.f, 24 et 32 du RGPD (pris ensemble), mais, pour ces trois dispositions, dans une mesure moindre que celle retenue par la Décision.

Les violations concernent donc un manquement à l'obligation de réaliser une AIPD (art. 35) et un manquement à l'obligation de mettre en œuvre des mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque (art. 32), différentes défaillances ayant été identifiées à ce égard. S'agissant de ce second manquement, la Cour relève qu'il s'agit d'un manquement à l'article 32, qui est la disposition-clé du RGPD à cet égard ; si la Décision cite également les articles 5.1.f et 24, il ne s'agit que de références accessoires. En particulier, l'invocation de l'article 5.1.f à l'appui des violations retenues, par la référence que cette disposition inclut, au titre des principes, aux mesures techniques et organisationnelles appropriées, a

manifestement un caractère accessoire, et ne change pas la nature de la violation, qui concerne l'absence de ces mesures techniques et organisationnelles appropriées pour garantir la sécurité des données.

La Cour considère que ces manquements (à l'article 35 et à l'article 32) doivent effectivement être considérés comme des manquements importants, dès lors en particulier que l'activité hospitalière de la Requérante l'amène à traiter des données de santé visées à l'article 9 du RGPD pour un nombre important de personnes. Aussi, la Chambre contentieuse a constaté que, même après avoir subi une première cyberattaque, la Requérante ne s'était pas (encore) mise en conformité avec le RGPD par la réalisation d'une AIDP et de mesures techniques et organisationnelles appropriées pour garantir la sécurité des données.

Au vu de ce qui précède, la Décision n'est pas critiquable en son principe en ce qu'elle décide d'imposer une amende administrative. La Chambre contentieuse a pu estimer qu'une amende était nécessaire pour son effet dissuasif. Elle est restée, ce faisant, dans les marges de son pouvoir d'appréciation. Infliger une amende constitue une mesure efficace de sanction et de prévention.

62. Il reste à examiner si le montant de l'amende est justifié, tenant compte des principes et règles applicables et rappelés ci-avant, en particulier le principe que l'amende doit être effective, proportionnée et dissuasive.

Le principe de proportionnalité exige que la mesure adoptée ne dépasse pas les limites de ce qui est nécessaire à la réalisation des objectifs légitimes poursuivis par la réglementation.

Dès lors que le respect de ces principes conditionne la légalité de l'amende, la Cour dispose d'un plein pouvoir pour apprécier le respect de ces principes et plus largement des conditions de l'article 83 du RGPD.

63. En ce qui concerne la fixation du montant de départ pour le calcul de l'amende administrative, la Décision a pris en compte l'article 83.5 du RGPD, vu la violation constatée à l'article 5.1.f, et dès lors le montant de départ plus élevé de plafond équivalent à 20.000.000 € ou 4% du chiffre d'affaires annuel mondial, le montant le plus élevé étant retenu, soit 20.000.000 €.

Cependant, comme indiqué ci-avant, la violation retenue à l'article 5.1.f n'avait pas de contenu propre indépendant de la violation de l'article 32 RGPD. Il y avait dès lors lieu de faire application de l'article 83.4. du RGPD, comme le soutient la Requérante en son douzième moyen à titre subsidiaire. Il ne peut en effet être permis à l'autorité de court-circuiter l'application de l'article 83.4 en retenant systématiquement et sans contenu propre une violation d'un principe énoncé à l'article 5 du RGPD, la plupart des violations pouvant toujours être rattachés à un de ces principes. Quant à la violation de l'article 24 du RGPD, elle n'a pas à être prise en considération, puisqu'elle n'est visée ni à l'article 83.4 ni à l'article 83.5 du RGPD et n'est dès lors pas susceptible de justifier une amende.

COVER 01-00004516182-0046-0052-01-02-1

En tout état de cause, calculer l'amende à partir du plafond repris à l'article 83.4. aboutit à une situation disproportionnée, tenant compte de ce que l'objet véritable de l'infraction est un manquement à l'article 32 RGPD.

Le montant de départ à prendre en considération comme point de départ pour le calcul de l'amende à infliger à la Requérante aurait dès lors dû être celui prévu à l'article 83.4. du RGPD : 2% du chiffre d'affaires annuel total de l'exercice précédent, soit 1.450.724,45 € (2 % de 72.536.222,71 €, chiffre d'affaires retenu par la Décision) ou 10.000.000 €, le montant le plus élevé de 10.000.000 € devant être retenu.

Le moyen est donc fondé en ce qu'il critique la Décision pour avoir pris comme point de départ le montant de 20.000.000 € pour démarrer le calcul du montant de l'infraction, et la Décision annulée en ce qu'elle est partie de ce montant, alors qu'il aurait dû s'agir du montant de 10.000 €.

64. S'agissant de la gravité de la violation, à juste titre et de manière adéquatement motivée – sous réserve de ce qui sera précisé ci-après, la Décision a retenu une gravité moyenne.

Quant aux dispositions du RGPD : il y a lieu de tenir compte de la violation des articles 32 et 35 (pas des articles 5.1.f et 24, comme indiqué précédemment) : il s'agit de dispositions importantes du RGPD pour assurer la sécurité du traitement des données.

Or, les enjeux de sécurité sont importants, la Requérante traitant, de par son activité hospitalière, des données de santé et données sensibles de ces patients, et ce à grande échelle (300.000 patients). Quant à la gravité du dommage, à raison la Décision retient un niveau de dommage modéré. La durée est aussi correctement appréciée (2 ans et 6 mois).

Par contre, s'agissant du caractère délibéré ou négligent, il n'y a pas, comme le relève la Décision, de caractère intentionnel, avec pour conséquence qu'il s'agit de négligence. A tort, la Décision retient que le caractère sérieux de la négligence renforcerait la gravité de la violation. La mention, à l'article 83.2.b du RGPD de la prise en compte du caractère intentionnel ou négligent implique une gravité plus grande pour l'infraction intentionnelle ; la négligence, qu'elle soit considérée comme « sérieuse » ou « légère » - vocables qui ne sont pas repris à l'article 83.2.b, n'est pas de nature à renforcer la gravité de la violation.

La Décision retient, pour la violation de gravité moyenne, un montant de départ de 15 % du montant maximal de départ.

Dès lors que la Décision a repris a tort la négligence, qualifiée de « sérieuse », comme caractère renforçant la gravité, il y a lieu de retenir une gravité moyenne légèrement inférieure à celle reprise

par la Décision attaquée, et de fixer à 13 % le pourcentage à prendre en considération du montant maximum de départ.

Soit 13 % de 10.000.000 € = 1.300.000 €.

66. La Décision fait ensuite application des Lignes directrices 04/2022 sur le calcul des amendes administratives de l'EDPB pour tenir compte d'un correctif tenant compte du montant du chiffre d'affaires du dernier exercice de la Requérante, soit 72.536.222,71 €.

Selon les Lignes directrices, le pourcentage à prendre en considération pour un chiffre d'affaires entre 50 et 100 millions d'EUR est de 8 à 20 %.

A l'estime de la Cour, dès lors que la Requérante exploite un hôpital et est constituée sous la forme d'une ASBL, il y avait lieu de prendre en compte le pourcentage le plus bas de la fourchette, s'agissant d'une entité dont le but n'est pas de faire du profit mais qui poursuit un but désintéressé.

Faisant application du pourcentage de 8%, le résultat est de 104.000 €.

L'application du pourcentage de 13 % aboutirait à un montant disproportionné.

S'agissant des circonstances atténuantes, la Décision retient à juste titre:

- Les mesures prises pour atténuer le dommage ;
- La crise sanitaire du COVID 19 qui a pu limiter les ressources et l'attention disponible pour assurer pleinement la conformité aux exigences du RGPD ;
- La crise énergétique et l'inflation confrontant les hôpitaux à des circonstances économiques exceptionnelles, et impactant la capacité pour la Requérante à disposer des moyens nécessaires pour renforcer les mesures de sécurité nécessaires à la protection des données.

Il y avait cependant d'autres éléments que la Chambre contentieuse aurait dû prendre en compte au titre de circonstances atténuantes additionnelles, comme l'invoquent les moyens examinés :

- Le dossier fait suite à la dénonciation opérée par la Requérante elle-même et celle-ci a coopéré parfaitement avec l'Autorité ;
- Les violations commises n'ont pas eu pour conséquences des avantages financiers pour la Requérante ;
- Le cœur de l'activité de la Requérante est les soins hospitaliers et non le traitement de données personnelles ; ce traitement n'est effectué que de manière accessoire pour permettre la bonne réalisation de son activité ;
- Le but désintéressé poursuivi par la Requérante ;
- Les ressources financières limitées de la Requérante, ses difficultés financières avérées, et la nécessité d'allouer ces ressources par priorité à la mise en conformité des traitements de données personnelles au RGPD, plutôt qu'au paiement d'une amende trop importante ;

- L'absence de code de conduite disponible pour le secteur hospitalier et l'absence de travail en amont effectué par l'APD pour aider les institutions hospitalières à réaliser les obligations qui leur incombent et le contenu précis des obligations mises à leur charge, en dépit du caractère sensible des données de santé.

Tenant compte de l'ensemble des éléments qui précèdent, le montant de l'amende infligé par la Décision (200.000 €) est manifestement disproportionné.

Ce montant dépasse les limites de ce qui était nécessaire aux fins d'assurer les objectifs de prévention et de sanction.

Partant, les moyens pris ensemble sont fondés dans cette mensure, et justifient l'annulation de la Décision en ce que celle-ci inflige une amende de 200.000 €.

67. En vertu de son pouvoir de pleine juridiction, la Cour des marchés peut, après avoir annulé la Décision du fait du caractère disproportionné de l'amende (cfr supra), procéder à un nouvel examen pour déterminer elle-même le montant de l'amende, par application des dispositions légales applicables, en particulier les articles 100 à 102 de la LCA et 83 du RGPD.

Au vu des éléments examinés ci-avant il se justifie, faisant application des critères prévus à l'article 83 d RGPD et à la lumières des Lignes directrices de l'EDPD, de fixer le montant de l'amende à 50.000 €.

QUATORZIEME MOYEN REQUERANTE : moyen pris de la violation de l'article 83.1. du RGPD : les ordres de mise en conformité ne constituent pas une sanction effective.
Quatorzième moyen APD.

Résumé des parties

68. La **Requérante** fait valoir que, les ordres de mise en conformité énoncés dans la Décision attaquée ne sont pas efficaces (i) parce qu'ils ne permettent pas à la Requérante de comprendre ce qui est attendu d'elle dans le cadre de cette mise en conformité et (ii) parce qu'elle avait déjà pris les mesures adéquates pour mettre ses traitements en conformité avec le RGPD et ce, avant que la Chambre contentieuse ne prenne la Décision attaquée.

69. Concernant l'analyse d'impact, l'**APD** fait valoir que même à les supposer complètes, les deux AIPD ont été effectuées bien après la Décision attaquée. En ce qui concerne le programme de formation/sensibilisation des employés au RGPD, la Requérante ne rapporte pas la preuve qu'un tel véritable programme aurait été mise en place avant ou après la date de l'offre de PWC (21 novembre 2022). Concernant le mot de passe, la requérante affirme avoir mis en route l'amélioration de ses mots de passe, sans preuve ni indication particulière quant à une période.

Discussion et décision par la Cour

70. Comme spécifié au § 205 de la Décision, les ordres de mise en conformité visent quatre injonctions distinctes :
- la réalisation d'une AIPD ;
- la mise en place d'une « politique claire et précise relatives à la sécurité de l'information et à la vie privée » ;
- la mise en place d'un « programme de formation / sensibilisation des employés au RGPD régulier » ;
- le renforcement de la longueur du mot de passe d'accès au dossier informatisé du patient.

71. La Cour a reconnu l'obligation pour la Requérante de réaliser une AIDP conformément à l'article 35 du RGPD (cfr supra, examen du septième moyen en sa première branche). L'ordre de mise en conformité visant la réalisation d'une telle AIPD est une sanction adéquate et effective au manquement constaté.

Le moyen ne permet pas de comprendre en quoi il critique la sanction en sus des critiques formulées au septième moyen, qui ont été écartées par la Cour.
La Requérante invoque d'ailleurs avoir fait réaliser depuis la décision deux AIPD, l'une pour l'usage de la messagerie électronique, et l'autre pour le dossier médical des patients. L'APD conteste le caractère probant des documents déposés (notamment au motif que ces documents ne sont pas datés et n'identifient pas leur auteur), mais la Cour n'est pas saisie de la question de savoir si l'ordre de conformité a bien été exécuté ou non.

Le moyen n'est pas fondé en ce qu'il critique le caractère effectif de l'ordre de conformité ou sa légalité.

72. S'agissant des ordres de mise en conformité concernant la mise en place d'une « politique claire et précise relative à la sécurité de l'information et de la vie privée » et d'un « programme de formation/sensibilisation des employés au RGPD régulier », ils se fondent sur des constats de violation qui sont annulés par la Cour. Par voie de répercussion, ils sont également annulés.

73. Enfin, le quatrième ordre de mise en conformité vise le renforcement du mot de passe d'accès au dossier informatisé du patient.

La Cour a reconnu la violation commise par la Requérante au vu du manque de robustesse prévu par sa politique de mot de passer pour les accès aux dossiers médicaux informatisés. L'ordre de mise en conformité constitue une sanction adéquate et effective à la violation constatée.

Le moyen ne permet pas de comprendre en quoi il critique la sanction en sus des critiques formulées au septième moyen en sa septième branche, qui ont été écartées par la Cour

Si la Requérante invoque avoir initié un processus de mise en place de renforcement de la robustesse des mots de passer puis l'avoir renforcé, l'examen du caractère adéquat ressortirait de la question de savoir si l'ordre de mise en conformité a été bien exécuté ou non, question dont la Cour n'est pas saisie par le présent recours.

CONCERNANT LES DEPENS

74. La Requérante obtient partiellement gain de cause dans son recours, ce qui justifie la compensation intégrale des dépens, chaque partie conservant les dépens exposés et aucune indemnité de procédure n'étant due entre les parties.

PAR CES MOTIFS,
LA COUR DES MARCHES,

Vu les dispositions de la loi du 15 juin 1935 sur l'emploi des langues en matière judiciaire,

Statuant contradictoirement,

Dit le recours recevable,

Le dit partiellement fondé,

Annule partiellement la décision n° 166/2024 quant au fond rendue le 17 décembre 2024 par la Chambre contentieuse de l'Autorité de protection des données dans le dossier DOS-2021-06114 en ce que :

- elle considère que la Requérante 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 des données (constat de violation n° 2, § 88 de la Décision) **et en ce qu'elle impose un ordre de mise en conformité** relatif à la mise en place d'une « politique claire et précise relative à la sécurité de l'information et de la vie privée « (§ 205, b) de la Décision et dispositif) ;
- elle considère que la Requérante 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 (§ 105 de la Décision, constat de violation n° 4, premier élément retenu), **et en ce qu'elle impose un ordre de mise en conformité** relatif à la mise en place d'un tel programme de formation (§ 205, c de la Décision et dispositif)
- elle considère que la Requérante 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 (§ 113 de la Décision, constat de violation n° 4, deuxième élément retenu.

Annule également ladite Décision en ce qu'elle impose une amende administrative d'un montant de 200.000 € à la Requérante,

Faisant usage de son pouvoir de pleine juridiction, fixe le montant de l'amende administrative à 50.000 € , pour violation des articles 32 et 35 du RGPD,

Déboute la Requérante du surplus de son recours,

Compense intégralement les dépens entre les parties,

Condamne l'ASBL [redacted] (aussi appelée « [redacted] ») à payer au profit du SPF Finances la moitié des droits de mise au rôle dus devant la cour d'appel, soit 200 €, conformément à l'article 269^2 § $1^{er,}$ du Code des droits d'enregistrement, d'hypothèque et de greffe,

Dit pour droit que l'APD est dispensée du paiement de l'autre moitié des droits de mise au rôle dus devant la cour d'appel, par l'effet des articles 2791, 1° et 161, 1°bis du Code des droits d'enregistrement, d'hypothèque et de greffe,

Ainsi jugé et prononcé à l'audience civile publique de la $19^{ème}$ chambre A de la cour d'appel de Bruxelles, section Cour des marchés, le 03 septembre 2025,

Où étaient présents :

C. VERBRUGGEN,	Conseiller, ff. président
A.-M. WITTERS,	Conseiller,
O. DUGARDYN,	Conseiller suppléant,
A. MONIN,	Greffier,

A. MONIN

O. DUGARDYN

A.-M WITTERS

C. VERBRUGGEN