



## Chambre Contentieuse

### Décision 52/2023 du 8 mai 2023

**Numéro de dossier : DOS-2023-01071**

**Objet : Plainte contre une commune pour consultation irrégulière du Registre national par un de ses agents**

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

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

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

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

Vu les pièces du dossier ;

#### **A pris la décision suivante concernant :**

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

**La défenderesse :** Commune Y, ci-après : « la défenderesse ».

## I. Faits et procédure

1. L'objet de la plainte concerne une consultation irrégulière du Registre national de la plaignante par un agent de la commune Y en date du 12 décembre 2022. La plaignante indique que l'agent qui a procédé à cette consultation aurait transmis son adresse à son ex petit ami, qui a ainsi pu se présenter à son domicile et la harceler.

La plaignante a envoyé plusieurs emails à la défenderesse (le 20,24 et 27 janvier 2023) afin de s'enquérir des raisons de cette consultation car elle indique n'avoir aucun lien (résidence ou professionnel) avec ladite commune.

Le 28 janvier 2023, une employée du Service population et état civil de la commune défenderesse lui répond que ce type de dossier est géré par le directeur adjoint du service population de la commune concernée. La plaignante explique que celui-ci l'aurait contacté par téléphone par la suite, en indiquant qu'un agent de la commune aurait bien procédé à la consultation du Registre national de la plaignante, sans pouvoir justifier la consultation. La plaignante reproche aussi au directeur adjoint du service en cause de ne pas l'avoir tenu informée des suites disciplinaires pour l'agent auteur de la consultation irrégulière, ce qui sort néanmoins de la compétence de l'APD et ne sera donc pas abordé dans la présente décision.

2. Le 6 mars 2023, la plaignante a introduit une plainte auprès de l'Autorité de protection des données contre la défenderesse.
3. Le 22 mars 2023, la plainte est déclarée recevable par le Service de Première Ligne sur la base des articles 58 et 60 de la LCA<sup>1</sup> et la plainte est transmise à la Chambre Contentieuse en vertu de l'article 62, § 1<sup>er</sup> de la LCA<sup>2</sup>.
4. En application de l'article 95 § 2, 3<sup>o</sup> de la LCA ainsi que l'article 47 du règlement d'ordre intérieur de l'APD, une copie du dossier peut être demandée par les parties. Si l'une des parties souhaite faire usage de la possibilité de consulter le dossier, celle-ci est tenue de s'adresser au secrétariat de la Chambre contentieuse, de préférence via l'adresse [litigationchamber@apd-gba.be](mailto:litigationchamber@apd-gba.be).

---

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

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

## **II. Motivation**

### **II.1. Quant à la qualité de responsable de traitement**

5. En application de l'article 4 § 1er LCA, l'Autorité de protection des données (APD) est responsable du contrôle des principes de protection des données contenus dans le RGPD et d'autres lois contenant des dispositions relatives à la protection du traitement des données à caractère personnel dont la loi du 8 août 1983 organisant un Registre national des personnes physique.
6. Conformément à l'article 4.7 du RGPD, il y a lieu de considérer comme responsable du traitement : « la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement ».
7. En l'occurrence, la Chambre Contentieuse constate que c'est bien la défenderesse qui détermine les finalités et les moyens du traitement. En effet, les consultations du Registre national sont effectuées uniquement dans le cadre des missions de la commune, bien que les finalités des consultations spécifiques qui ont lieu en l'espèce ne fait pas partie de ces missions. C'est par ailleurs celle-ci qui met à disposition les moyens pour effectuer ce traitement. Elle doit donc être considérée comme responsable de traitement.
8. Il convient également de souligner que, comme le rappelle la CJUE dans son arrêt *Wirtschaftsakademie* du 5 juin 2018, « la notion de « responsable du traitement » vise l'organisme qui, « seul ou conjointement avec d'autres » détermine les finalités et les moyens du traitement de données à caractère personnel, cette notion ne renvoie pas nécessairement à un organisme unique et peut concerner plusieurs acteurs(...)». Que la défenderesse soit responsable de traitement pour les consultations de ses employés au Registre national ne signifie donc pas, dans le cas d'espèce, qu'elle seule corresponde à cette qualité. Il convient en effet de distinguer les consultations au Registre national dans le cadre des finalités de la défenderesse des consultations abusives opérées à des fins privées par un agent communal.
9. Comme indiqué ci-dessous, bien que l'agent communal ait utilisé les moyens mis à sa disposition par la défenderesse, dans la mesure où l'agent communal a opéré des consultations irrégulières en dehors du cadre de ses fonctions en tant qu'employé.e de la défenderesse, l'agent doit être considéré comme responsable de traitement pour ces consultations abusives spécifiquement.

10. Comme l'indique l'EDPB<sup>3</sup>, ceci n'exempte néanmoins en rien la défenderesse, en tant que responsable du traitement des consultations au Registre national, de son obligation d'assurer la sécurité des traitements. Cet aspect est développé ci-dessous.
11. Par ailleurs, l'agent de la défenderesse n'ayant pas été visé par la plainte déposée auprès de l'APD, cet agent n'est pas parti à la présente procédure. Pour cette raison, la Chambre contentieuse n'effectuera pas de constats additionnels à son égard.

## **II.2. Rappel de l'obligation de sécurité dans le chef du responsable de traitement**

12. L'accès à l'information contenue dans le Registre national constitue un traitement de données à caractère personnel au sens de l'article 4.2 du RGPD. Dès lors, ce traitement, est soumis aux différentes obligations du RGPD. La Chambre Contentieuse rappelle qu'en sa qualité de responsable de traitement, la défenderesse est tenue de mettre en œuvre les principes de protection des données et doit être en mesure de démontrer que ceux-ci sont respectés (principe de responsabilité – article 5.2. du RGPD).
13. Elle doit par ailleurs, toujours en sa qualité de responsable de traitement, mettre en œuvre toutes les mesures nécessaires à cet effet (article 24 du RGPD). La Chambre Contentieuse insiste, comme elle a déjà eu l'occasion de le rappeler dans de précédentes décisions prises<sup>4</sup> à l'encontre de mandataires publics, sur le fait que le secteur public, doit, de manière générale, être vecteur d'exemple dans les mesures qu'il adopte pour garantir le respect du droit fondamental à la protection des données personnelles.

### **II.2.1. Les contours de l'obligation de sécurité**

14. Sur base de l'article 5.1.f RGPD, les données à caractère personnel doivent être traitées de façon à garantir une sécurité appropriée, « 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 ».
15. En l'absence de mesures appropriées pour sécuriser les données à caractère personnel des personnes concernées, l'effectivité des droits fondamentaux à la vie privée et à la protection des données à caractère personnel ne peut être garantie, à fortiori au vu du rôle crucial joué par les technologies de l'information et de la communication dans notre société.

---

<sup>3</sup> EDPB "Lignes directrices 07/2020 concernant les notions de responsable du traitement et de sous-traitant dans le RGPD », Version 2.0 Adoptées le 7 juillet 2021

<sup>4</sup> Voy notamment décisions 10/2019 et 11/2019 de la Chambre Contentieuse du 25 novembre 2019 aux termes desquelles la Chambre Contentieuse rappelle que la qualité de mandataire public des responsables de traitement mis en cause aurait dû s'accompagner d'un comportement exemplaire au regard du respect de la législation, en ce compris celle relative à la protection des données personnelles.

16. Il convient de relever que les principes d' « intégrité, confidentialité et disponibilité » repris à l'article 5,1,f) sont désormais érigés dans le RGPD au même rang que les principes fondamentaux de licéité, transparence, loyauté.
17. Les obligations des responsables de traitement quant à la sécurité des traitements reposent sur l'article 32 du RGPD.
18. Les composantes classiques des recommandations en termes de sécurité de l'information, telles que préconisées par la suite ISO27xxx sont la confidentialité des données, leur intégrité et leur disponibilité. A celles-ci s'ajoute la notion d'imputabilité, « qui permet de pouvoir identifier, pour toutes les actions accomplies, les personnes, les systèmes ou les processus qui les ont initiées (identification) et de garder trace de l'auteur et de l'action (traçabilité) ». L'imputabilité s'exprime notamment de façon concrète par la tenue d'un registre des log files selon le principe de journalisation des accès.
19. La journalisation consiste donc à enregistrer des informations pertinentes concernant les évènements d'un système informatique (accès au système ou à un de ses dossiers, modification d'un fichier, transfert de données...) dans des fichiers appelés « log files ». Les informations reprises sont entre autres les données consultées, la date, le type d'évènement, les données permettant d'identifier l'auteur de l'évènement, ainsi que le motif de cet accès. Ceci permet notamment d'identifier toute consultation des données personnelles abusive ou pour une finalité non légitime, ou encore de déterminer l'origine d'un accident.
20. Bien que la journalisation ne soit pas expressément mentionnée dans le RGPD, la tenue d'un journal des log files constitue une mesure technique et organisationnelle envisagée dans l'article 32 RGPD. Elle constitue une bonne pratique, recommandée au responsable de traitement lorsque cette mesure est adaptée aux risques liés aux caractéristiques du traitement.
21. L'institution prédécesseur de l'APD (la Commission de la Vie Privée –CPVP ci-dessous-) indiquait déjà dans ses Lignes directrices pour la sécurité de l'information de données à caractère personnel ainsi que dans ses Recommandations aux villes et communes concernant les registres de logs IT que la journalisation constitue un élément incontournable de toute politique de sécurité de l'information, en ce qu'elle permet de traçabilité des accès aux systèmes informatiques.
22. Cette pratique a par ailleurs été consacrée par le législateur qui a intégré cette obligation dans l'article 17 de la loi du 8 aout 1983 organisant un Registre national des personnes physiques. Cet article indique :
 

« Chaque autorité publique, organisme public ou privé ayant obtenu l'autorisation d'accéder aux informations du Registre national des personnes physiques, en ce compris les services

de police, ainsi que ceux de la Justice cités aux articles 5 et 8 doit être en mesure de pouvoir justifier les consultations effectuées, que celles-ci se fassent par un utilisateur individuel ou par un système informatique automatique. A cet effet, afin d'assurer la traçabilité des consultations, chaque utilisateur tient un registre des consultations. Ce registre indique l'identification de l'utilisateur individuel ou du processus ou du système qui a accédé aux données, les données qui ont été consultées, la façon dont elles ont été consultées, à savoir en lecture ou pour modification, la date et l'heure de la consultation ainsi que la finalité pour laquelle les données du Registre national des personnes physiques ont été consultées.»

(La Chambre Contentieuse souligne)

### **II.2.2. Lien entre les obligations de sécurité des responsables de traitement et les principes de responsabilité**

23. L'article 32 du RGPD doit être lu conjointement avec les articles 5.2 et 24 du RGPD, le responsable de traitement étant soumis au principe de responsabilité.
24. Il incombe donc au responsable de traitement de démontrer la mise en place de mesures techniques et organisationnelles appropriées, de façon transparente et traçable, permettant en cas de contrôle d'apporter la preuve des garanties appliquées.
25. Le principe de responsabilité, lu en conjonction avec le principe de transparence (article 5.1.a RGPD), permet aux personnes concernées d'exercer leurs droits et de contrôler la conformité des traitements opérés sur leurs données à caractère personnel. Elle permet ainsi d'assumer la responsabilité.
26. Le considérant 63 du RGPD ajoute en outre à cela que ce droit d'accès doit être considéré comme un mécanisme de contrôle : *"Une personne concernée devrait avoir le droit d'accéder aux données à caractère personnel qui ont été collectées à son sujet et d'exercer ce droit facilement et à des intervalles raisonnables, afin de prendre connaissance du traitement et d'en vérifier la licéité."*
27. Ces principes de responsabilité et de transparence s'articulent avec l'article 15 du RGPD, qui garantit le droit d'accès de la personne concernées à ses données personnelles traitées. La CPVP concluait déjà à l'égard de la journalisation, de façon univoque :
 

« *Un fichier de journalisation incomplet et une absence de mention du motif de la consultation constituent une atteinte à l'exercice utile du droit d'accès et de contrôle dont dispose la personne concernée. Cela compromet également l'exercice des autres droits tels que le droit de rectification (article 16 du RGPD), le droit à l'oubli (article 17 du RGPD), et le droit à la limitation de l'utilisation de données traitées de façon illicite (article 18 du RGPD).* »

(p10)

28. La Chambre Contentieuse recommande la tenue d'un registre journal des log files en tant que bonne pratique, dans la mesure où la journalisation est utile pour tout responsable de traitement, en ce qu'elle permet d'assurer la matérialisation du principe de disponibilité, lui-même étroitement lié aux principes de confidentialité et d'intégrité des données.
29. La Chambre contentieuse souligne par ailleurs, comme indiqué supra, qu'il s'agit d'une obligation légale inscrite dans la loi organisant le Registre national, telle que modifiée par la Loi du 25 novembre 2018 portant des dispositions diverses concernant le Registre national et les registres de population qui est entrée en vigueur le 24 décembre 2018. Par ailleurs, parmi les mesures de sécurité adaptées destinées à garantir la confidentialité des données, un responsable de traitement tel que la défenderesse est nécessairement tenu de mettre en place des mesures de sécurité organisationnelles et techniques qui garantissent un contrôle des accès<sup>5</sup> : en d'autres termes, seules les personnes qui, dans l'exercice de leur fonction propre, ont besoin d'accéder à telle ou telle donnée doivent pouvoir bénéficier des accès nécessaires à cet effet.
30. La Chambre Contentieuse rappelle à cet égard l'article 5.1.b) RGPD qui consacre le principe de finalité, soit l'exigence que les données soient collectées pour des finalités déterminées, explicites et légitimes et ne soient pas traitées ultérieurement d'une manière incompatible avec ces finalités. A cet égard, la défenderesse est autorisée à consulter le Registre national pour des finalités déterminées conformément à la Loi du 8 août 1983 organisant un Registre national des personnes physiques.
31. Le responsable de traitement doit donc s'assurer que les données à caractère personnel ne sont accessibles qu'aux personnes et aux applications qui en ont explicitement l'autorisation. Il convient d'attribuer à chaque personne son propre compte et l'accès aux données à caractère personnel devrait être exclusivement autorisé en appliquant les principes du besoin d'en connaître. Ces personnes devraient uniquement avoir accès à la fonctionnalité ou aux données dont elles ont besoin aux fins de l'exécution des tâches qui leur sont dévolues et ce, dans le respect du principe de finalité.

---

<sup>5</sup> Voy. notamment les Mesures de référence en matière de sécurité applicables à tout traitement de données à caractère à personnel édictées par la Commission de la protection de la vie privée : <https://www.autoriteprotectiondonnees.be/lexique/mesures-de-referance>

« Sécurisation logique des accès

L'organisme doit s'assurer que les données à caractère personnel ne soient accessibles, conformément à leur classification, qu'aux personnes et aux applications qui en ont explicitement l'autorisation. Il maintiendra à jour une liste actualisée des différentes personnes habilitées à accéder et traiter ces données et de leurs pouvoirs respectifs (création, consultation, modification, destruction). Ces différentes autorisations doivent être traduites en dispositifs techniques et contrôles d'accès aux différents éléments informatiques (programmes, procédures, éléments de stockage, équipements de télécommunication, etc.) intervenant dans le traitement des données à caractère personnel. Ces dispositions techniques doivent inclure les activités en amont (développement applicatif) et en aval (gestion des exemplaires de sauvegarde). Si le niveau de sécurité l'impose, l'identification des intervenants sera complétée par une procédure d'authentification. »

32. Il incombe donc à la défenderesse de garantir que l'accès au Registre national demeure limité aux finalités pour lesquelles cet accès a été autorisé. Il lui incombe également d'être en mesure de le démontrer. Le respect du principe de finalité, pilier de la protection des données, ne peut en effet pas être vérifié si les agents d'une structure telle la défenderesse n'enregistrent pas le motif de la consultation qu'ils opèrent. Il est tout aussi essentiel à cet égard que conformément à l'article 24 du RGPD, la défenderesse dispose d'un mécanisme de contrôle adéquat garantissant que ses agents habilités consultent le Registre national dans le cadre de ces seules finalités. La défenderesse doit disposer d'une application informatique qui permette de légitimer chaque consultation effectuée par son personnel et démontre ainsi que la consultation a eu lieu dans le cadre de l'exercice des tâches du membre du personnel qui a effectué la consultation.
33. La Chambre contentieuse rappelle qu'elle s'est par le passé exprimée au sujet de l'accès aux données du Registre national. Ainsi, la décision 19/2020<sup>6</sup> impose notamment que le responsable de traitement ayant accès aux données du Registre national mette en place un contrôle des accès, et garantisse que l'accès au Registre national demeure limité aux finalités pour lesquelles cet accès a été autorisé. Il lui incombe également d'être en mesure de le démontrer. Ces obligations sont déduites par la Chambre contentieuse notamment des articles 5.1.b et f, 5.2., 24, 32 du RGPD et de l'article 17 de la Loi du 8 août 1983 organisant un Registre national des personnes physiques.
34. La Chambre Contentieuse estime que sur la base des faits susmentionnés, il y a lieu de conclure que la défenderesse peut avoir commis une violation des articles 32 et 5.1.f) du RGPD, ainsi que de l'article 17 de la loi du 8 août 1983 organisant un Registre national des personnes physiques, ce qui justifie qu'en l'occurrence, l'on procède à la prise d'une décision conformément à l'article 95, §1<sup>er</sup>, 4<sup>o</sup> de la LCA, plus précisément d'ordonner de se conformer aux principes de sécurité du traitement (article 32 du RGPD) et de responsabilité du responsable du traitement (article 24 du RGPD).
35. La présente décision est une décision *prima facie* prise par la Chambre Contentieuse conformément à l'article 95 de la LCA sur la base de la plainte introduite par le plaignant/la plaignante, dans le cadre de la « *procédure préalable à la décision de fond* »<sup>7</sup> et pas une décision sur le fond de la Chambre Contentieuse au sens de l'article 100 de la LCA.
36. La présente décision a pour but d'informer la défenderesse, présumée responsable du traitement, du fait que celle-ci peut avoir commis une violation des dispositions du RGPD, afin de lui permettre d'encore se conformer aux dispositions précitées.

---

<sup>6</sup> Décision 19/2020 du 29 avril 2020 (<https://www.autoriteprotectiondonnees.be/publications/decision-quant-au-fond-n-19-2020.pdf>)

<sup>7</sup> Section 3, Sous-section 2 de la LCA (articles 94 à 97 inclus).



37. Si toutefois la défenderesse n'est pas d'accord avec le contenu de la présente décision *prima facie* et estime qu'elle peut faire valoir des arguments factuels et/ou juridiques qui pourraient conduire à une autre décision, elle peut adresser à la Chambre Contentieuse une demande de traitement sur le fond de l'affaire via l'adresse e-mail [litigationchamber@apd-gba.be](mailto:litigationchamber@apd-gba.be), et ce dans le délai de 30 jours après la notification de la présente décision. Le cas échéant, l'exécution de la présente décision est suspendue pendant la période susmentionnée.
38. En cas de poursuite du traitement de l'affaire sur le fond, en vertu des articles 98, 2° et 3° *juncto* l'article 99 de la LCA, la Chambre Contentieuse invitera les parties à introduire leurs conclusions et à joindre au dossier toutes les pièces qu'elles jugent utiles. Le cas échéant, la présente décision est définitivement suspendue.
39. Dans une optique de transparence, la Chambre Contentieuse souligne enfin qu'un traitement de l'affaire sur le fond peut conduire à l'imposition des mesures mentionnées à l'article 100 de la LCA<sup>8</sup>

### **III. Publication de la décision**

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

---

<sup>8</sup> Art. 100. § 1<sup>er</sup>. La chambre contentieuse a le pouvoir de

- 1° classer la plainte sans suite ;
- 2° ordonner le non-lieu ;
- 3° prononcer la suspension du prononcé ;
- 4° proposer une transaction ;
- 5° formuler des avertissements et des réprimandes ;
- 6° ordonner de se conformer aux demandes de la personne concernée d'exercer ses droits ;
- 7° ordonner que l'intéressé soit informé du problème de sécurité ;
- 8° ordonner le gel, la limitation ou l'interdiction temporaire ou définitive du traitement ;
- 9° ordonner une mise en conformité du traitement ;
- 10° ordonner la rectification, la restriction ou l'effacement des données et la notification de celles-ci aux récipiendaires des données ;
- 11° ordonner le retrait de l'agrément des organismes de certification ;
- 12° donner des astreintes ;
- 13° donner des amendes administratives ;
- 14° ordonner la suspension des flux transfrontières de données vers un autre État ou un organisme international ;
- 15° transmettre le dossier au parquet du Procureur du Roi de Bruxelles, qui l'informe des suites données au dossier ;
- 16° décider au cas par cas de publier ses décisions sur le site internet de l'Autorité de protection des données.

**PAR CES MOTIFS,**

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

- D'imposer un avertissement pour violation de l'article 32 du RGPD et de l'article 17 de la loi du 8 août 1983 organisant un Registre national des personnes physiques, sur la base de l'article 95 § 1, 4° LCA, si la défenderesse ne se conforme pas à l'avenir aux principes de sécurité et responsabilité quant aux accès par ses agents au Registre national (notamment par la mise en place d'un contrôle des accès, visant à garantir que l'accès au Registre national demeure limité aux finalités pour lesquelles cet accès a été autorisé, ainsi que d'être en mesure de le démontrer)
- D'ordonner à la défenderesse d'informer par e-mail l'Autorité de protection des données (Chambre Contentieuse) de la suite qui est donnée à cette décision, dans le même délai, via l'adresse e-mail [litigationchamber@apd-gba.be](mailto:litigationchamber@apd-gba.be) ; et
- si la défenderesse ne se conforme pas en temps utile à ce qui lui est demandé ci-dessus, de traiter d'office l'affaire sur le fond, conformément aux **articles 98 e.s.** de la LCA.

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

Un tel recours peut être introduit au moyen d'une requête interlocutoire qui doit contenir les informations énumérées à l'article 1034<sup>ter</sup> du Code judiciaire<sup>9</sup>. La requête interlocutoire doit être

---

<sup>9</sup> La requête contient à peine de nullité:

1° l'indication des jour, mois et an;

2° les nom, prénom, domicile du requérant, ainsi que, le cas échéant, ses qualités et son numéro de registre national ou numéro d'entreprise;

3° les nom, prénom, domicile et, le cas échéant, la qualité de la personne à convoquer;

4° l'objet et l'exposé sommaire des moyens de la demande;

5° l'indication du juge qui est saisi de la demande;

6° la signature du requérant ou de son avocat.

déposée au greffe de la Cour des Marchés conformément à l'article 1034<sup>quinquies</sup> du C. jud.<sup>10</sup>, ou via le système d'information e-Deposit du Ministère de la Justice (article 32<sup>ter</sup> du C. jud.).

(sé). Hielke HUMANS

Président de la Chambre Contentieuse

---

<sup>10</sup> La requête, accompagnée de son annexe, est envoyée, en autant d'exemplaires qu'il y a de parties en cause, par lettre recommandée au greffier de la juridiction ou déposée au greffe.