Autorité de protection des données
Gegevensbeschermingsautoriteit

Chambre Contentieuse

Décision quant au fond 141/2021 du 16 décembre 2021

Numéro de dossier : DOS-2020-03763

Objet : L'exercice des droits de la personne concernée à l'égard des systèmes d'information d'une banque.

La Chambre Contentieuse de l'Autorité de protection des données, constituée de Monsieur Hielke Hijmans, président, et de Messieurs Dirk Van Der Kelen et Frank De Smet, membres ;

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

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

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

Vu les pièces du dossier ;

a pris la décision suivante concernant :

Le défendeur : la banque Y, représentée par Me Erik Valgaeren et Me Carolien Michielsen, ci-après "le défendeur"

I. Faits et procédure

A. *Enquête du Service d'Inspection*

1. Le 22 avril 2020, le Comité de direction de l'Autorité de protection des données (ci-après l'APD) a décidé de saisir le Service d'Inspection de l'APD de l'affaire sur la base de l'article 63, 1° de la LCA.

   Suite à la décision n° 01/2019 prise par la Chambre Contentieuse le 15 mai 2019 et l'arrêt consécutif de la Cour des marchés du 9 octobre 2019, le Comité de direction a en effet constaté qu'il y avait des indices sérieux de pratiques pouvant donner lieu à des violations des principes fondamentaux de la protection des données à caractère personnel. Le Comité de direction a dès lors saisi le Service d'Inspection du dossier en demandant de mener une enquête sur la mesure dans laquelle les systèmes d'information du défendeur permettent l'exercice des droits de la personne concernée, en particulier le doit de rectification (article 16 du RGPD). Cela signifie que le Service d'Inspection est saisi afin de vérifier si les systèmes d'information du défendeur sont conformes aux exigences posées par le RGPD au niveau de l'exercice des droits dont dispose toute personne concernée[1] en sa qualité de client du défendeur.

2. Le Service d'Inspection a transmis son rapport du 23 mars 2021 à la Chambre Contentieuse sur la base de l'article 91, § 2 de la LCA, impliquant la saisine de la Chambre Contentieuse en vertu de l'article 92, 3° de la LCA.

B. *Procédure devant la Chambre Contentieuse*

3. Le 6 avril 2021, la Chambre Contentieuse décide, en vertu de l'article 95, § 1er, 1° et de l'article 98 de la LCA, que le dossier peut être traité sur le fond.

4. Le même jour, le défendeur est informé par courrier recommandé de cette décision ainsi que du rapport d'inspection et de l'inventaire des pièces du dossier qui a été transmis à la Chambre Contentieuse par le Service d'Inspection. De même, le défendeur est informé des dispositions de l'article 98 de la LCA et, en vertu de l'article 99 de la LCA, il est informé des délais pour introduire ses conclusions. La date limite pour la réception des conclusions en réponse du défendeur a été fixée au 28 mai 2021.

5. Le 10 mai 2021, le défendeur demande une copie du dossier (art. 95, § 2, 3° de la LCA), qui lui est transmise le 12 mai 2021. Le défendeur accepte également de recevoir toutes les communications

[1] La décision n° 01/2019 du 15 mai 2019 concerne par contre uniquement la sauvegarde des droits d'un seul plaignant déterminé dont les données à caractère personnel ont été traitées par le défendeur, étant donné que la Chambre Contentieuse n'avait été saisie que pour ce traitement dans la plainte.

relatives à l'affaire par voie électronique et manifeste son intention de recourir à la possibilité d'être entendu, ce conformément à l'article 98 de la LCA.

6. Le 28 mai 2021, la Chambre Contentieuse reçoit les conclusions en réponse du défendeur dans lesquelles il est demandé, en ordre principal, de constater qu'il n'y a pas de violation des articles 5.1 c), d) et f), 5.2, 12, 16, 24, 25, 30.1, 31, 32, 38.3 et 38.6 du RGPD et, en ordre subsidiaire, de tenir compte des circonstances atténuantes lors de l'imposition d'une sanction.

7. Le 14 juillet 2021, les parties sont informées du fait que l'audition aura lieu le 30 septembre 2021.

8. Le 30 septembre 2021, le défendeur est entendu par la Chambre Contentieuse et a ainsi l'occasion d'avancer ses arguments. La Chambre Contentieuse décide de mettre l'affaire en continuation afin de permettre au défendeur, après l'échéance du délai du 15 novembre 2021 qu'il a avancé lui-même, à savoir la date à laquelle l'introduction de signes diacritiques dans les noms et les prénoms dans ses applications devrait être réalisée, de venir expliquer le nouveau système informatique. Une nouvelle audition sera programmée à cet effet peu après cette date.

9. Le 1er octobre 2021, le défendeur est informé du fait que l'audition visant à mettre l'affaire en continuation aura lieu le 22 novembre 2021.

10. Le 12 octobre 2021, le procès-verbal de l'audition du 30 septembre 2021 est transmis au défendeur, conformément à l'article 54 du règlement d'ordre intérieur de l'APD. Le défendeur a ainsi l'occasion de faire ajouter ses éventuelles remarques en annexe au procès-verbal.

11. Le 19 octobre 2021, la Chambre Contentieuse reçoit quelques remarques du défendeur au sujet du procès-verbal, qu'elle décide de reprendre dans sa délibération une fois que la séance fixée au 22 novembre 2021 aura eu lieu.

12. Le 22 novembre 2021, le défendeur est entendu par la Chambre Contentieuse et il explique la réalisation de l'introduction de signes diacritiques dans les noms et les prénoms dans ses applications.

13. Le 23 novembre 2021, le procès-verbal de l'audition du 22 novembre 2021 est soumis au défendeur, conformément à l'article 54 du Règlement d'ordre intérieur de l'APD. Le défendeur se voit ainsi offrir l'opportunité de faire ajouter ses éventuelles remarques à cet égard en annexe du procès-verbal, sans que cela implique une réouverture des débats.

14. Le 23 novembre 2021, la Chambre Contentieuse a fait connaître au défendeur son intention de procéder à l'imposition d'une amende administrative ainsi que le montant de celle-ci, afin de donner au défendeur l'occasion de se défendre avant que la sanction soit effectivement infligée.

15. Le 29 novembre 2021, la Chambre Contentieuse reçoit les remarques à l'égard du procès-verbal de l'audition qui a eu lieu le 22 novembre 2021, remarques que la Chambre Contentieuse reprend dans sa délibération.

16. Le 14 décembre 2021, la Chambre Contentieuse reçoit la réaction du défendeur concernant l'intention d'infliger une amende administrative, ainsi que le montant de celle-ci. Le défendeur avance qu'un certain nombre de circonstances atténuantes qui ont été exposées dans les conclusions pour Y Belgique et lors de l'audition, n'ont pas été prises en considération par la Chambre Contentieuse étant donné qu'elles ne figurent pas dans le formulaire de sanction et que l'amende envisagée est disproportionnellement élevée par rapport à la décision quant au fond n° 18/2020 du 28 avril 2020 pour une violation identique.

II. Motivation

17. La Chambre Contentieuse évalue ci-après chacune des constatations reprises dans le rapport du Service d'Inspection à la lumière des moyens avancés à cet égard par le défendeur.

a) Principe d'exactitude (article 5.1 d) du RGPD), de responsabilité (article 5.2 du RGPD), d'information transparente, de communication et autres modalités pour l'exercice des droits de la personne concernée (article 12 du RGPD), de droit de rectification (article 16 du RGPD), de protection des données dès la conception et de protection des données par défaut (article 25 du RGPD) et d'obligation de coopération (article 31 du RGPD)

18. Le premier élément faisant l'objet d'une enquête du Service d'Inspection concerne l'évaluation de la mesure dans laquelle le défendeur a apporté les modifications nécessaires afin d'implémenter les signes diacritiques dans ses systèmes ICT.

19. Le Service d'Inspection constate que le défendeur ne peut pas créer d'image technique du système en termes de planning pour l'implémentation de signes diacritiques dans le système ICT actuel (applications + mainframe) et les éventuels premiers résultats témoignant des efforts réalisés. Par ailleurs, le Service d'Inspection constate également que le défendeur reste dans la "phase exploratoire" d'étude préalable et de discussion, sans vouloir atteindre des objectifs et des résultats concrets.

20. Le Service d'Inspection en arrive à la conclusion que le défendeur commet une violation des articles 5.1 d, 5.2, 12, 16, 25 et 31 du RGPD car il ne veut ou ne peut pas soumettre un planning concret avec des résultats concrets et ne veut ou ne peut pas non plus démontrer de modifications techniques du système ayant un impact positif sur la demande initiale de la personne concernée. Selon le Service d'Inspection, la situation depuis la décision prise par la Chambre Contentieuse le 15 mai 2019 (à l'exception de la réalisation d'un travail d'étude préalable (faisabilité)) est restée inchangée et ne s'est donc pas améliorée.

21. Le Service d'Inspection fait valoir les considérations suivantes à cet égard :

    - Le défendeur a des applications IT et des systèmes de bases de données (environ 150) dont le système client central qui est un système mainframe qui a été mis en service en 1995.

Ce système client central supporte uniquement l'EBCDIC ("extended binary-coded decimal interchange code"). Bien que les signes diacritiques aient entre-temps été ajoutés au tableau EBCDIC, le défendeur n'a apporté aucune modification dans le système client central. En 2020, le défendeur utilise encore un système informatique qui date de 1995 et qui ne permet pas d'exercer le droit de rectification.

- En ce qui concerne le nombre d'applications sous-jacentes qui interagissent avec le système client central, qui nécessitent une modification suite à l'introduction des signes diacritiques, le Service d'Inspection constate que le défendeur mentionne 150 applications dans son courrier initial du 6 novembre 2019 et ce n'est que le 2 novembre 2020 qu'il est en mesure de fournir une liste correspondant au nombre précis tel que mentionné le 6 novembre 2019, complétée par la bonne dénomination technique du système et le filtrage des doublons. Le Service d'Inspection fait remarquer à cet égard que le défendeur répondait souvent que l'analyse n'était pas encore clôturée, ce qui est étrange étant donné le nombre de mois écoulés, le nombre de membres du personnel, les moyens financiers et les possibilités du défendeur.
- En ce qui concerne les grands systèmes très anciens au sujet desquels le défendeur affirme le 6 novembre 2019 que leur adaptation durera 18 mois, le Service d'Inspection constate que le défendeur ne fournit que le 2 novembre 2020 une liste décrivant ces systèmes et les citant spécifiquement.
- En enquêtant sur le 'change management' et le plan d'approche visant à procéder à l'implémentation des propositions techniques, le Service d'Inspection tente de se faire une idée du développement des processus et de la manière dont les implémentations sont réalisées au sein du défendeur. Le Service d'Inspection constate que le défendeur indique le 16 septembre 2020 que les modifications devant être effectuées en vue de l'introduction de lettres avec accents se feront selon le principe AGILE en vigueur au sein de Y, ce qui implique que le défendeur résoudra la limitation des lettres avec accents par petites étapes synoptiques.

Le 12 octobre 2020, le défendeur indique avoir pris des initiatives afin de reprendre les signes diacritiques dans le système client central ; une approche en 4 phases est suivie et à ce moment, les phases 1 et 2 sont traitées :

1) analyse de tous les systèmes et applications susceptibles d'être touchés ;
2) adaptations de ces systèmes dans l'environnement de test et test de ceux-ci de manière individuelle à l'égard du traitement de signes diacritiques ;
3) réalisation de chaînes de tests afin de garantir la cohérence des applications ;
4) réalisation concrète des modifications.

Le 2 novembre 2020, le défendeur documente la manière dont AGILE a été traduit au sein de son organisation et fournit des informations quant à l'étude de faisabilité sous forme de deux schémas concernant l'approche de testing.

Le Service d'Inspection en arrive à la conclusion qu'il est étrange de ne disposer que de peu d'informations structurées et génériques pour suivre cette adaptation de manière globale. À l'exception d'informations générales au sujet de l'approche AGILE et de la phase d'étude préliminaire, le défendeur ne peut pas fournir d'informations démontrant une éventuelle avancée ou des résultats concrets pouvant avoir un impact positif sur la personne concernée et l'exercice de ses droits.

- Suite à l'examen du design technique, le rapport d'inspection contient les schémas techniques concernant le design architectural où le défendeur indique chaque fois si, et le cas échéant dans quelle mesure, des modifications peuvent avoir un impact sur chacune des parties, ce aussi bien pour le système client central, les technologies d'appui et sous-jacentes – middleware, applications Z mainframe, applications Z non mainframe, les applications non mainframe – que pour les canaux et applications front-end.

Articles 5.1. d), 12 et 16 du RGPD

22. Le défendeur avance que les articles 5.1 d), 12 et 16 du RGPD sont respectés, ce qu'il argumente comme suit :

- L'exercice des droits de la personne concernée est facilité conformément à l'article 12 du RGPD du fait que les clients peuvent adapter eux-mêmes leurs données via les applications pour opérations bancaires par Internet ou les faire adapter par des collaborateurs du front-office. La déclaration de confidentialité mentionne également les coordonnées utiles pour exercer le droit de rectification. En outre, il existe également un fil conducteur interne et une documentation des procédures pour l'exercice des droits des personnes concernées. Les processus nécessaires ont aussi été implémentés afin de traiter adéquatement les demandes d'exercice des droits.

- Le droit de rectification (article 16 du RGPD) est respecté pour toutes les demandes d'adaptation ou de rectification. L'impossibilité à laquelle le défendeur fait face pour donner suite à la demande d'adaptation est limitée au traitement de signes diacritiques dans un nom.

- - La réalisation d'un projet IT complexe avec des adaptations de nombreux systèmes, qui requiert beaucoup de temps et d'investissements pour répondre à une minorité absolue de demandes de rectification, ne doit pas être considérée selon le défendeur comme une mesure raisonnable au sens de l'article 5.1 d) du RGPD.

- Le défendeur indique que l'arrêt de la Cour des marchés du 9 octobre 2019 est encore pendant devant la Cour de cassation et que dans l'attente du prononcé, on ne peut pas simplement affirmer

que les articles 5.1 d), 12 et 16 du RGPD ne sont pas respectés en raison du manque d'indication de signes diacritiques.

23. Les conclusions du défendeur indiquent qu'il était prévu au départ d'implémenter les signes diacritiques dans ses systèmes ICT dans le cadre du projet ICT "UNITE" déjà en cours en 2019 au sein du Groupe Y, lequel visait à harmoniser intégralement les systèmes et applications des entités Y en Belgique avec celles des entités Y aux Pays-Bas ; le projet UNITE s'est toutefois révélé trop ambitieux et en 2020, le défendeur a dû réaliser seul, donc sans Y Pays-Bas, les adaptations techniques du système utiles. Sur la base de cette déclaration, la Chambre Contentieuse constate que l'intention de reprendre les signes diacritiques dans les applications du défendeur existait, mais que cela ne s'est pas concrétisé du fait de la dissociation du défendeur au sein du projet UNITE. Le défendeur affirme à présent dans les conclusions que l'intégration des signes diacritiques dans les applications suppose le dépassement des limites du raisonnable, tandis que l'article 5.1 d) du RGPD requiert uniquement que le défendeur prenne toutes les mesures raisonnables pour que les données à caractère personnel qui sont inexactes, eu égard aux finalités pour lesquelles elles sont traitées, soient effacées ou rectifiées sans tarder.

24. Sur la base du rapport d'inspection, la Chambre Contentieuse constate que le système client central, qui constitue le cœur de la banque du fait que les données client y sont enregistrées de manière centrale et en sont extraites par les systèmes connexes, est un système mainframe qui a été mis en service en 1995. Bien que les signes diacritiques aient entre-temps été ajoutés au tableau EBCDIC, le défendeur n'a pas apporté de modifications dans le système client central qui supporte EBCDIC. Cela signifie que le défendeur n'a pas exploité cette possibilité pour adapter son système.

25. Bien que le caractère raisonnable de la réalisation de cette mesure soit contesté par le défendeur, la Chambre Contentieuse estime qu'il est normal que le client dont les données à caractère personnel sont traitées dans le cadre de sa relation financière avec la banque s'attende à ce que son nom soit indiqué correctement, précisément eu égard à l'importance de l'exactitude des données lors de la fourniture de services et produits financiers. La Chambre Contentieuse se réfère aussi à cet égard à l'arrêt de la Cour des marchés du 9 octobre 2019 qui précise que l'on peut attendre d'une institution bancaire qui fonctionne correctement qu'elle dispose d'un programme informatique qui répond aux normes actuelles, incluant le droit précité à une orthographe correcte du nom. Et la Cour d'ajouter que le droit de rectification est un droit fondamental[2]. Il est dès lors

[2] L'arrêt de la Cour des marchés est rédigé dans les termes suivants :

"[...]

Le fait que cela nécessiterait techniquement un "effort" pour utiliser un programme informatique qui met les accents sur les lettres majuscules n'est pas grave et n'est pas pertinent.

"Affirmer à présent (en 2019 !) que l'adaptation d'un programme informatique nécessiterait plusieurs mois et/ou un surcoût financier pour l'établissement bancaire, ne permet pas à la SA Y BELGIQUE d'ignorer les droits de la personne concernée. Les droits qui sont attribués à la personne sont assimilables à des engagements de résultat dans le chef de celui qui traite les données à caractère personnel.

raisonnable que la banque prenne les mesures qui sont à sa disposition afin de traiter le nom des clients avec des signes diacritiques et d'adapter ainsi aux possibilités actuelles le système mainframe qui est en service depuis 1995. En ce qui concerne l'argument du défendeur selon lequel une telle adaptation non seulement de son système client central mais aussi des systèmes sous-jacents ou connexes requiert beaucoup de temps et d'investissements, ce qui ne peut pas être considéré comme raisonnable, la Chambre Contentieuse fait remarquer que cela est généralement propre à tout changement fondamental de systèmes informatiques, ce qui vaut d'autant plus lorsqu'il s'agit d'anciens systèmes comme en l'espèce. La nécessité de consacrer du temps et des investissements pour des systèmes informatiques appropriés afin de pouvoir traiter des signes diacritiques ne se limite pas (contrairement à ce que prétend le défendeur) à une minorité absolue de demandes de rectification mais est nécessaire dans l'intérêt de tout client dont le nom contient des signes diacritiques. Le point de départ doit en effet être que le défendeur, tout comme n'importe quel responsable du traitement, mette tout en œuvre pour traiter des données exactes et n'adopte pas une attitude passive et donc qu'il n'attende pas une demande d'un client pour faire modifier son nom pour entreprendre une action visant à réaliser cette adaptation.

26. La Chambre Contentieuse estime dès lors que l'impossibilité du défendeur de procéder jusqu'à présent à la rectification de nom de clients qui demandent l'indication de signes diacritiques dans leur nom constitue une **violation de l'article 5.1 d) du RGPD**. Cela constitue également une **violation de l'article 16 du RGPD**, étant donné que le défendeur n'est pas en état de respecter entièrement le droit de rectification. Le défendeur affirme que toutes les demandes d'adaptation ou de rectification sont réalisées, sauf la demande d'adaptation de signes diacritiques. Cela amène la Chambre Contentieuse à conclure que le défendeur ne donne pas suite à tout exercice du droit de rectification. Le droit de rectification doit cependant être respecté dans toutes ses facettes.

27. Lors de la détermination de la sanction de ces violations, la Chambre Contentieuse tient toutefois compte de la déclaration du défendeur de s'engager à avoir réalisé, d'ici le 15 novembre 2021, toutes les adaptations nécessaires pour pouvoir intégrer les signes diacritiques dans les noms et les prénoms dans ses applications. Dans le cadre de cet engagement de résultat, le défendeur formule deux mises en garde dont la Chambre Contentieuse prend acte :

    1° Conformément à la norme industrielle en vigueur au niveau mondial, les signes diacritiques ne sont pas repris sur les cartes bancaires. Si le défendeur le faisait, cela pourrait poser problème lors de l'utilisation de la carte bancaire, tant en ligne qu'hors ligne. En ce qui concerne les paiements électroniques (SEPA), toutes les banques belges ont également convenu de se limiter à l'ensemble de signes standard, sans signes diacritiques.

On peut attendre d'un établissement bancaire qui fonctionne bien que – lorsqu'il utilise un programme informatique -, il en utilise un qui répond aux normes actuelles, incluant le droit précité à une orthographe correcte du nom. Le droit de rectification est un droit fondamental.

[…]"

2° L'indication de signes diacritiques sur les extraits imprimés de cartes de crédit ne sera disponible qu'à une date ultérieure.

Lors de l'audition du 22 novembre 2021, le défendeur donne une présentation qui témoigne suffisamment du fait que les démarches utiles ont été entreprises pour traiter les signes diacritiques dans les noms des clients, de sorte que la Chambre Contentieuse peut constater une avancée sur ce point. En ce qui concerne spécifiquement le plaignant dans la décision n° 01/2019 du 15 mai 2019, le défendeur démontre également que le signe diacritique dans son nom est traité.

28. En ce qui concerne l'article 12 du RGPD, la Chambre Contentieuse constate que le défendeur démontre suffisamment qu'il y a une communication transparente à l'égard des clients afin de les informer de l'exercice de leurs droits, et que les moyens nécessaires sont mis à disposition pour exercer ces droits, le défendeur facilitant ainsi l'exercice de ces droits. Il ne ressort en outre pas du rapport d'inspection que le défendeur ne mènerait pas une communication transparente (article 12.1 du RGPD). Le rapport d'inspection indique seulement que pour le défendeur, il n'est pas possible au niveau technique du système de donner suite à une demande de rectification concernant les signes diacritiques, mais que cela n'empêche pas que le défendeur facilite bel et bien l'exercice des droits de ses clients (article 12.2 du RGPD) via les applications de banque par Internet ou avec l'aide des collaborateurs du front-office, même si le défendeur n'est pas en mesure d'y donner une suite appropriée et de procéder immédiatement à la rectification dans la mesure où la demande porte sur les signes diacritiques (article 16 du RGPD). Il en résulte que l'on ne peut pas constater de violation de l'article 12 du RGPD.

29. En ce qui concerne l'affirmation du défendeur selon laquelle la Chambre Contentieuse ne pourrait pas procéder à la constatation d'une violation des articles 5.1 d), 12 et 16 du RGPD pour cause d'absence d'indication de signes diacritiques, en raison de la procédure pendante devant la Cour de cassation introduite par le défendeur à l'encontre de l'arrêt de la Cour des marchés rendu suite à la décision n° 01/2019[3] de la Chambre Contentieuse, la Chambre Contentieuse souligne que le recours en cassation constitue un recours extraordinaire qui n'a pas d'effet suspensif. Cela signifie que dans l'attente du prononcé de la Cour de cassation, l'arrêt de la Cour des marchés produit pleinement ses effets et que le Service d'Inspection pouvait saisir la Chambre Contentieuse via le rapport d'inspection du 23 mars 2021 et que dès lors, la Chambre Contentieuse peut prendre à présent cette décision quant au fond.

Article 25 du RGPD

30. Le défendeur affirme que le Service d'Inspection constate une violation présumée de l'article 25 du RGPD mais qu'il n'explique pas en quoi cette violation consiste.

[3] Décision n° 01/2019 du 15 mai 2019 relative à une plainte pour non-respect de la demande de correction de l'orthographe du nom.

31. La Chambre Contentieuse estime que le rapport d'inspection démontre clairement que pour son système client central, le défendeur utilise encore jusqu'à présent un mainframe qui a été mis en service en 1995 et nonobstant la possibilité technique d'y intégrer et d'y traiter les signes diacritiques, il a choisi de ne pas harmoniser son système en ce sens. Conformément à l'article 25 du RGPD, l'état de la technique qui permet le traitement de signes diacritiques requiert que le défendeur prenne les mesures techniques et organisationnelles adéquates afin de réaliser efficacement les principes de protection des données, dont le principe d'exactitude, et d'intégrer les garanties nécessaires dans le traitement pour respecter les prescriptions du RGPD et pour protéger les droits des personnes concernées.

32. Le défendeur indique que l'article 25 du RGPD cite également, comme critère pour déterminer les mesures appropriées, les coûts de mise en œuvre ainsi que les risques afférents au traitement, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques. Le défendeur prétend à cet égard qu'il n'y a *aucun risque* en ce qui concerne l'identification de la personne quant à l'usage concret d'un certain nom sans indication du signe diacritique spécifique. En outre, la réalisation d'un projet IT très complexe avec des adaptations de nombreux systèmes requiert beaucoup de temps et d'investissements afin de pouvoir répondre à une minorité absolue de demandes de rectification et de ce fait, selon le défendeur, le *risque est extrêmement limité* en termes de gravité et de probabilité pour les droits et libertés des personnes physiques.

33. L'affirmation du défendeur selon laquelle il n'y a pas de risque d'identification de la personne concernée en l'absence de traitement des signes diacritiques et que le risque est extrêmement limité vu le faible nombre de demandes de rectification concernant les signes diacritiques ne peut pas impliquer, selon la Chambre Contentieuse, que le défendeur reste totalement en défaut, comme en l'espèce, de prendre la moindre mesure pour pouvoir répondre à d'éventuelles demandes de rectification.

34. Par ailleurs, le défendeur se réfère aux lignes directrices 4/2019 *relatives à l'article 25 - Protection des données dès la conception et protection des données par défaut*[4] qui prévoient au niveau de l'exactitude des données que les exigences posées par l'article 5.1 d) du RGPD doivent être considérées en fonction des risques et des conséquences de l'utilisation concrète des données. Le défendeur estime pouvoir en déduire que la mesure consistant en l'intégration des signes diacritiques dans ses systèmes n'est pas proportionnelle aux risques pour la personne concernée. Le défendeur oublie toutefois le fait que, en ce qui concerne la protection des données dès la conception et à la protection des données par défaut en termes d'exactitude, les lignes directrices y relatives prévoient spécifiquement en ce qui concerne l'effacement/la rectification que le responsable du traitement efface ou rectifie sans délai les données inexactes. Les lignes directrices confirment ainsi ce que prévoit l'article 5.1 d) du RGPD, à savoir que tout responsable du traitement

[4] https://edpb.europa.eu/system/files/2021-04/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_fr.pdf.

a l'obligation d'effacer ou de rectifier sans tarder les données inexactes et qu'il n'appartient pas au responsable du traitement d'accéder ou non à une demande d'effacement ou de rectification de données inexactes en raison de considérations financières ou d'une analyse de risques.

35. Du fait que le défendeur n'a pas adapté ses systèmes IT afin de permettre le traitement de signes diacritiques dans le nom des clients si une demande est introduite en ce sens, il y a **violation de l'article 25 du RGPD**. Le défendeur fait valoir qu'entre-temps, à savoir depuis la décision 01/2019 du 15 mai 2019 et le rapport d'inspection en question, il a déjà fourni de nombreux efforts pour rendre ses systèmes conformes au RGPD pour ce qui est du traitement de signes diacritiques, ce qui constitue également un élément important pour déterminer la sanction de cette violation. Cela ne peut toutefois pas donner lieu à une annulation rétroactive de la violation.

36. Vu les efforts fournis entre-temps par le défendeur ainsi que la gravité et les risques limités pour les droits fondamentaux des personnes en question, à la lumière du considérant 75 du RGPD, la Chambre Contentieuse décide, malgré qu'elle a constaté des violations des articles 5.1.d), 16 et 25 du RGPD, de ne pas procéder à l'imposition d'une sanction pour ces violations. Elle ordonne dès lors un non-lieu, en vertu de l'article 100, § 1er, 2° de la LCA.

Articles 5.2 et 31 du RGPD

37. Dans le rapport du Service d'Inspection, il apparaît à plusieurs reprises qu'il a fallu adresser plusieurs lettres au défendeur pour qu'il apporte des réponses concrètes aux questions posées, en conséquence de quoi le Service d'Inspection en déduit que le défendeur n'a pas respecté sa responsabilité et son obligation de coopération. Le Service d'Inspection s'étonne également qu'il y ait peu d'informations structurées et génériques pour suivre les adaptations de manière globale. À l'exception d'informations générales au sujet de l'approche AGILE et de la phase d'étude préliminaire, le Service d'Inspection estime que le défendeur ne peut pas fournir d'informations démontrant une éventuelle avancée ou des résultats concrets pouvant avoir un impact positif sur la personne concernée et l'exercice de ses droits et libertés.

38. Sur la base des pièces fournies par le défendeur, la Chambre Contentieuse doit toutefois constater que par le biais de la documentation requise, le défendeur peut démontrer dans quelle mesure le RGPD est respecté. Non seulement le défendeur a mis à disposition un fil conducteur et une documentation internes des procédures pour l'exercice des droits des personnes concernées, mais il a également mis spécifiquement à disposition une documentation relative au projet IT dédié à l'implémentation des signes diacritiques ainsi que les processus qui démontrent l'avancement du projet. Ainsi, le défendeur a documenté quelles étapes ont déjà été entreprises ainsi que celles qu'il entreprendra encore à l'avenir. Pour expliquer la durée nécessaire pour répondre aux questions posées par le Service d'Inspection au cours des différentes phases, le défendeur déclare qu'une analyse approfondie était requise afin de déterminer quelles applications peuvent être impactées par l'ajout de signes diacritiques et que cela n'était pas possible immédiatement. Le défendeur

affirme qu'il fallait du temps pour réaliser des analyses et des tests afin de réaliser ensuite les adaptations de manière contrôlée, sans mettre en péril la stabilité de ses systèmes. À cet égard, la Chambre Contentieuse constate sur la base des pièces que le défendeur a apporté suffisamment de documentation démontrant incontestablement l'avancée dans le dossier et les résultats concrets, de sorte **qu'aucune violation de l'article 5.2 du RGPD** ne peut être établie.

39. La Chambre Contentieuse a également évalué les constatations du Service d'Inspection à la lumière de l'obligation de coopération du défendeur et constate que le Service d'Inspection n'a pas démontré suffisamment que le défendeur n'avait pas tenté par le biais de lettres de réponse de répondre de manière détaillée et circonstanciée aux questions posées. En outre, le défendeur s'est déclaré à plusieurs reprises disposé à engager une concertation, en complément de cette approche. On ne peut donc pas établir qu'il n'a pas tenu compte de l'obligation de coopération avec l'autorité de contrôle.

40. La Chambre Contentieuse estime donc qu'**aucune violation de l'article 31 du RGPD** ne peut être constatée. Ce jugement se base sur des constatations de faits, rendant inutile un jugement de principe dans cette affaire concernant la portée de l'obligation de coopération.

b) Principe de minimisation des données (article 5.1 c) du RGPD), d'intégrité et de confidentialité (article 5.1 f) du RGPD), de responsabilité (article 5.2 du RGPD), de responsabilité du responsable du traitement (article 24 du RGPD), de protection des données dès la conception et de protection des données par défaut (article 25 du RGPD) et de sécurité du traitement (article 32 du RGPD)

41. Le Service d'Inspection constate que le défendeur utilise le nom de famille du plaignant[5] dans :

    - des notes internes pour le "Data Council" et des présentations de ce dernier
    - l'échange d'e-mails et des tests ICT

    qui concernent le programme ICT relatif à l'utilisation des signes diacritiques.

42. Le Service d'Inspection en conclut que cette activité de traitement du défendeur constitue une violation des articles 5.1 c) et f), 5.2, 24, 25 et 32 du RGPD, conclusion qui est basée sur la considération que l'utilisation du nom de famille du plaignant n'est pas nécessaire pour la finalité pour laquelle il est traité et peut donc être évitée. Le nom du projet ou de l'affaire pourrait porter un autre nom et le nom de famille du plaignant n'a aucune valeur ajoutée. Selon le Service d'Inspection, il y a divers mots dans d'autres langues avec des signes diacritiques qui peuvent être utilisés à cet effet, l'utilisation du nom de famille du plaignant peut être stigmatisante et du fait de sa diffusion au sein de son organisation, le défendeur n'a pas de contrôle à cet égard. Le rapport d'inspection

[5] Le Service d'Inspection se réfère au plaignant dans la décision n° 01/2019 du 15 mai 2019

conclut que le fait d'utiliser le nom de famille comme "personne de test" ou comme "affaire" n'est pas proportionné :

- à l'application des principes de base de "minimisation des données" et d' "intégrité et de confidentialité" ;
- aux mesures techniques ou organisationnelles appropriées à prendre ;
- à la garantie de confidentialité, d'intégrité, de disponibilité et de résilience de ses systèmes de traitement et de ses services ;
- à l'obligation de discrétion contractuelle (bancaire) ou au traitement discret des données à caractère personnel en tant que banque à l'égard du client.

43. La Chambre Contentieuse affirme que le nom de famille du plaignant dans la décision n° 01/2019 du 15 mai 2019 constitue bel et bien une donnée à caractère personnel au sens de l'article 4.1) du RGPD, étant donné que le plaignant est identifiable à l'aide de la décision n° 01/2019 prise par la Chambre Contentieuse et de l'arrêt de la Cour des marchés du 9 octobre 2019, dans lesquels le défendeur était chaque fois partie et que l'identité du plaignant lui était donc connue. Il en résulte que le plaignant peut être identifié directement à l'aide seulement de son nom de famille au sein de l'organisation du défendeur, étant donné qu'ils étaient tous deux partie dans le litige. Selon la Chambre Contentieuse, l'utilisation du nom de famille en tant que nom de projet doit être considérée comme un traitement basé sur l'intérêt légitime du défendeur (article 6.1 f) du RGPD).

44. Conformément à l'article 6.1.f) du RGPD et à la jurisprudence de la Cour de Justice de l'Union européenne (ci-après "la Cour"), trois conditions cumulatives doivent être remplies pour qu'un responsable du traitement, c'est-à-dire le défendeur, puisse valablement invoquer *ce fondement de licéité, "à savoir, premièrement, la poursuite d'un intérêt légitime par le responsable du traitement ou par le ou les tiers auxquels les données sont communiquées, deuxièmement, la nécessité du traitement des données à caractère personnel pour la réalisation de l'intérêt légitime poursuivi et, troisièmement, la condition que les droits et les libertés fondamentaux de la personne concernée par la protection des données ne prévalent pas" (arrêt "Rigas"*[6]).

45. En d'autres termes, afin de pouvoir invoquer le fondement de licéité de l' "intérêt légitime" conformément à l'article 6.1.f) du RGPD, le responsable du traitement doit démontrer que :

    - les intérêts qu'il poursuit avec le traitement peuvent être reconnus comme légitimes (le "test de finalité") ;

    - le traitement envisagé est nécessaire pour réaliser ces intérêts (le "test de nécessité") ; et

[6] CJUE, 4 mai 2017, C-13/16, Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde contre Rīgas pašvaldības SIA „Rīgas satiksme", considérant 28. Voir également CJUE, 11 décembre 2019, C-708/18,TK c/ Asociaţia de Proprietari bloc M5A-ScaraA, considérant 40.

- la pondération de ces intérêts par rapport aux intérêts, libertés et droits fondamentaux des personnes concernées pèse en faveur du responsable du traitement (le "test de pondération").

46. En ce qui concerne la première condition (le "test de finalité"), la Chambre Contentieuse estime que la finalité qui consiste à exécuter tant la décision précitée de la Chambre Contentieuse que l'arrêt de la Cour des marchés[7] peut être qualifiée comme étant poursuivie en vue d'un intérêt légitime. Conformément au considérant 47 du RGPD, l'intérêt que le défendeur poursuivait en tant que responsable du traitement peut en soi être considéré comme légitime. La première condition reprise à l'article 6.1.f) du RGPD est donc remplie.

47. Afin de remplir la deuxième condition, il faut démontrer que le traitement est nécessaire pour la réalisation des finalités poursuivies. Cela signifie plus précisément qu'il faut se demander si le même résultat ne peut pas être atteint avec d'autres moyens, sans traitement de données à caractère personnel ou sans traitement substantiel inutile pour la personne concernée.

48. Étant donné que le défendeur était chaque fois partie dans la procédure devant la Chambre Contentieuse et la Cour des marchés, l'identité du plaignant était déjà connue au sein d'un cercle limité de personnes de l'organisation du défendeur.

49. En outre, le défendeur déclare que le nom de famille a été utilisé dans des documents purement internes et confidentiels au sein du Data Council composé seulement de 7 membres ainsi que dans quelques e-mails limités aux personnes strictement nécessaires impliquées dans le projet. Il ne ressort d'aucune pièce que le traitement du nom de famille du plaignant aurait été inutilement invasif pour la personne concernée. La Chambre Contentieuse estime ainsi que le défendeur n'a pas traité le nom de famille de la personne concernée au mépris du principe de minimisation des données, de sorte que la deuxième condition est remplie.

50. Afin de vérifier si la troisième condition de l'article 6.1.f) du RGPD - ce qu'on appelle le "test de pondération" entre les intérêts du responsable du traitement d'une part et les libertés et droits fondamentaux de la personne concernée d'autre part - peut être remplie, conformément au considérant 47 du RGPD, il faut d'abord tenir compte des attentes raisonnables de la personne concernée. Il faut plus spécialement évaluer si *"la personne concernée peut raisonnablement s'attendre, au moment et dans le cadre de la collecte des données à caractère personnel, à ce que celles-ci fassent l'objet d'un traitement à une fin donnée"*[8].

[7] Voir dans le même sens la décision quant au fond 35/2020 du 30 juin 2020, point 28.

[8] Considérant 47 du RGPD.

51. Cet aspect est également souligné par la Cour dans son arrêt "TK c/ Asociaţia de Proprietari bloc M5A-ScaraA" du 11 décembre 2019[9], qui précise ce qui suit :

"Sont également pertinentes aux fins de cette pondération les attentes raisonnables de la personne concernée à ce que ses données à caractère personnel ne seront pas traitées lorsque, dans les circonstances de l'espèce, cette personne ne peut raisonnablement s'attendre à un traitement ultérieur de celles-ci."

52. Il résulte tant de la décision n° 01/2019 prise par la Chambre Contentieuse le 15 mai 2019 que de l'arrêt de la Cour des marchés du 9 octobre 2019 que le défendeur devait adapter ses applications, du moins en ce qui concerne le traitement de signes diacritiques dans le nom de famille de la personne concernée. Cela implique nécessairement que la personne concernée pouvait raisonnablement s'attendre[10] à ce que son nom de famille soit utilisé au sein de l'organisation du défendeur afin de répondre aux exigences posées dans la décision précitée de la Chambre Contentieuse et dans celle de la Cour des marchés.

53. L'ensemble des éléments précités amène la Chambre Contentieuse à conclure que le défendeur a traité le nom de famille de la personne concernée de manière légitime au sein de son organisation en vertu de l'article 6.1 f) du RGPD et qu'aucun élément n'est avancé pour affirmer que le défendeur aurait agi contrairement aux exigences du RGPD, de sorte que dans le chef du défendeur, **aucune violation des articles 5.1 c) et f), 5.2, 24, 25 et 32 du RGPD** n'a été commise.

c) Position du délégué à la protection des données (article 38.3 et 38.6 du RGPD)

54. En ce qui concerne la position du délégué à la protection des données, le rapport du Service d'Inspection constate qu'il y a un conflit d'intérêts dans son chef et que celui-ci ne fait pas rapport directement au niveau le plus élevé de l'organe de direction.

55. En ce qui concerne l'exigence de rapport direct au niveau le plus élevé de la direction (article 38.3 du RGPD), il est souligné dans la défense que le délégué à la protection des données rapporte à

---

[9] CJUE, 11 décembre 2019, C-708/18,TK c/ Asociaţia de Proprietari bloc M5A-ScaraA, considérant 58.

[10] Considérant 47 du RGPD. *Les intérêts légitimes d'un responsable du traitement, y compris ceux d'un responsable du traitement à qui les données à caractère personnel peuvent être communiquées, ou d'un tiers peuvent constituer une base juridique pour le traitement, à moins que les intérêts ou les libertés et droits fondamentaux de la personne concernée ne prévalent, compte tenu des attentes raisonnables des personnes concernées fondées sur leur relation avec le responsable du traitement. Un tel intérêt légitime pourrait, par exemple, exister lorsqu'il existe une relation pertinente et appropriée entre la personne concernée et le responsable du traitement dans des situations telles que celles où la personne concernée est un client du responsable du traitement ou est à son service. En tout état de cause, l'existence d'un intérêt légitime devrait faire l'objet d'une évaluation attentive, notamment afin de déterminer si une personne concernée peut raisonnablement s'attendre, au moment et dans le cadre de la collecte des données à caractère personnel, à ce que celles-ci fassent l'objet d'un traitement à une fin donnée. Les intérêts et droits fondamentaux de la personne concernée pourraient, en particulier, prévaloir sur l'intérêt du responsable du traitement lorsque des données à caractère personnel sont traitées dans des circonstances où les personnes concernées ne s'attendent raisonnablement pas à un traitement ultérieur. Étant donné qu'il appartient au législateur de prévoir par la loi la base juridique pour le traitement des données à caractère personnel par les autorités publiques, cette base juridique ne devrait pas s'appliquer aux traitements effectués par des autorités publiques dans l'accomplissement de leurs missions. Le traitement de données à caractère personnel strictement nécessaire à des fins de prévention de la fraude constitue également un intérêt légitime du responsable du traitement concerné. Le traitement de données à caractère personnel à des fins de prospection commerciale peut être considéré comme étant réalisé pour répondre à un intérêt légitime.* [soulignement propre].

l'Executive Committee, appelé aussi Comité de direction, et ce via le Chief Risk Officer (CRO) qui siège lui-même dans l'Executive Committee, à savoir l'organe le plus élevé. Le défendeur souligne que la ligne de rapport part bien directement du délégué à la protection des données à l'Executive Committee. Le rapport à un organe ne peut se faire que via une personne physique, à savoir en l'espèce le CRO qui sert de point d'accès à cet organe. Le défendeur justifie ce choix du CRO du fait qu'il est le membre de l'Executive Committee qui est l'interlocuteur privilégié du Risk Committee qui prend connaissance de tous les problèmes importants liés à la vie privée.

56. Le délégué à la protection des données est lui-même membre permanent du Data Council, qui est un sous-comité délégué et un prolongement de l'Executive Committee, les décisions du Data Council étant contraignantes pour l'Executive Committee. Le défendeur souligne que la présence du délégué à la protection des données dans le Data Council constitue une forme de rapport au niveau le plus élevé.

57. Le défendeur ajoute également que l'Executive Committee est un organe collégial, le CEO ayant une seule voix dans le processus décisionnel, tout comme tous les autres membres de cet organe. Le défendeur souligne lors de l'audition que le DPO ne doit pas faire rapport à l'individu le plus élevé, à savoir le CEO, au sein de l'organe le plus élevé, mais que le rapport au niveau le plus élevé suffit. En outre, tous les autres membres de l'Executive Committee, dont aussi le CEO, sont responsables de départements qui traitent des données. Il en résulte selon le défendeur que l'on ne peut pas prétendre qu'un certain membre de l'Executive Committee serait plus neutre que les autres membres.

58. Sur la base des pièces étayant l'explication donnée par le défendeur, la Chambre Contentieuse estime que l'on ne peut établir **aucune violation de l'article 38.3 du RGPD**.

59. En ce qui concerne le constat du Service d'Inspection selon lequel il y a un conflit d'intérêts dans le chef du délégué à la protection des données (article 38.6 du RGPD) du fait qu'il est également chef des services Operational Risk Management (ORM), Information Risk Management (IRM) et Special Investigation Unit (SIU), le défendeur avance que le chef de ces services n'a pas de compétence de décision au niveau des finalités et des moyens des traitements opérationnels de données à caractère personnel, mais uniquement une compétence d'avis et de contrôle.

60. Lors de l'audition, la Chambre Contentieuse a examiné l'impact que le délégué à la protection des données a sur le processus décisionnel en raison de ses autres fonctions.

61. La Chambre Contentieuse constate que le défendeur insiste dans ses conclusions sur les compétences purement d'avis et de contrôle de chacun des trois services, à savoir Operational Risk Management, Information Risk Management et Special Investigation Unit. Le défendeur estime pouvoir ainsi affirmer que le délégué à la protection des données n'a pas de tâches (aussi via ses fonctions dans chacun des services en question) en vertu desquelles il pourrait prendre des

décisions quant à la finalité et aux moyens d'un quelconque traitement de données à caractère personnel.

62. La Chambre Contentieuse estime qu'il n'est pas démontré ainsi que le délégué à la protection des données, qui est également chef de service de chacun de ces services et y endosse donc une position à responsabilités, n'exerce aucune tâche qui soit incompatible avec sa position en tant que délégué à la protection des données.

63. La Chambre Contentieuse fait remarquer dans ce cadre que le rôle de conseil et de contrôle des départements en tant que tels ne signifie pas qu'ils ne définissent pas la finalité et les moyens de traitements de données.

64. La Chambre Contentieuse doit évaluer comment et dans quelle mesure est assurée l'indépendance du délégué à la protection des données à l'égard de chacun de ces trois départements (dont il est chef de service).

65. Le défendeur désigne donc lui-même une même personne physique en tant que responsable de chacun des trois départements et en tant que délégué à la protection des données. Cette responsabilité pour chacun de ces trois départements implique incontestablement que cette personne, en cette qualité, détermine les finalités et les moyens du traitement de données à caractère personnel au sein de ces trois départements et donc est responsable des processus de traitement de données qui relèvent du domaine Operational Risk Management, Information Risk Management et Special Investigation Unit, comme cela a été constaté dans le rapport d'inspection.

66. Les Lignes directrices du Groupe 29 concernant les délégués à la protection des données[11] expliquent que le délégué à la protection des données ne peut exercer au sein de l'organisme une fonction qui l'amène à déterminer les finalités et les moyens du traitement de données à caractère

---

[11] *L'article 38, paragraphe 6, autorise les DPD à "exécuter d'autres missions et tâches". Il exige toutefois que l'organisme veille à ce que "ces missions et tâches n'entraînent pas de conflit d'intérêts".*

L'absence de conflit d'intérêts est étroitement liée à l'obligation d'agir en toute indépendance. Bien que les DPD soient autorisés à exercer d'autres fonctions, un DPD ne peut se voir confier d'autres missions et tâches qu'à condition que celles-ci ne donnent pas lieu à un conflit d'intérêts. Cela signifie en particulier que le DPD ne peut exercer au sein de l'organisme une fonction qui l'amène à déterminer les finalités et les moyens du traitement de données à caractère personnel. En raison de la structure organisationnelle spécifique de chaque organisme, cet aspect doit être étudié au cas par cas.

En règle générale, parmi les fonctions susceptibles de donner lieu à un conflit d'intérêts au sein de l'organisme peuvent figurer les fonctions d'encadrement supérieur (par exemple, directeur général, directeur opérationnel, directeur financier, médecin-chef, responsable du département marketing, responsable des ressources humaines ou responsable du service informatique), mais aussi d'autres rôles à un niveau inférieur de la structure organisationnelle si ces fonctions ou rôles supposent la détermination des finalités et des moyens du traitement. En outre, il peut également y avoir conflit d'intérêts, par exemple, si un délégué à la protection des données externe est appelé à représenter le responsable du traitement ou le sous-traitant devant les tribunaux dans des affaires ayant trait à des questions liées à la protection des données.

En fonction des activités, de la taille et de la structure de l'organisme, il peut être de bonne pratique pour les responsables du traitement ou les sous-traitants : • de recenser les fonctions qui seraient incompatibles avec celle de DPD ; • d'établir des règles internes à cet effet, afin d'éviter les conflits d'intérêts ; • d'inclure une explication plus générale concernant les conflits d'intérêts ; • de déclarer que leur DPD n'a pas de conflit d'intérêts en ce qui concerne sa fonction de DPD, dans le but de mieux faire connaître cette exigence ; • de prévoir des garanties dans le règlement intérieur de l'organisme et de veiller à ce que l'avis de vacance pour la fonction de DPD ou le contrat de service soit suffisamment précis et détaillé pour éviter tout conflit d'intérêts. Dans ce contexte, il convient également de garder à l'esprit que les conflits d'intérêts peuvent prendre différentes formes selon que le DPD est recruté en interne ou à l'extérieur.

WP243Rev01, paragraphe 3.5, soulignement par la Chambre Contentieuse. Ces lignes directrices ont été ratifiées par le Comité européen de la protection des données (EDPB).

personnel. Il s'agit donc d'un conflit d'intérêts substantiel. Le rôle de responsable d'un service n'est donc pas conciliable avec la fonction de délégué à la protection des données qui doit pouvoir exercer ses tâches en toute indépendance. Le cumul, dans le chef d'une même personne physique, de la fonction de responsable de chacun des trois services en question distinctement d'une part et de la fonction de délégué à la protection des données d'autre part prive chacun de ces trois services de toute possibilité de contrôle indépendant par le délégué à la protection des données. En outre, le cumul de ces fonctions peut avoir pour effet que le secret et la confidentialité envers les membres du personnel, en vertu de l'article 38.5 du RGPD, ne puissent pas être suffisamment garantis.

67. Le défendeur tente de réfuter l'existence d'un conflit d'intérêts dans le chef du délégué à la protection des données en affirmant que les services IRM, ORM et SIU font partie de la fonction de deuxième ligne et comprennent uniquement des fonctions de surveillance et de contrôle. Selon le défendeur, le chef de ces services, qui est également délégué à la protection des données, n'a pas de compétence de décision au niveau des finalités et des moyens des traitements opérationnels de données à caractère personnel, mais uniquement une compétence de conseil et de contrôle. Pour cette argumentation, le défendeur estime trouver un appui dans la décision quant au fond n° 56/2021 du 26 avril 2021.

68. Comme déjà défini dans les Lignes directrices du Groupe 29 concernant les délégués à la protection des données[12], la Chambre Contentieuse estime que l'évaluation de tout conflit d'intérêts doit se faire au cas par cas, au vu de l'organisation structurelle spécifique de toute organisation. La Chambre Contentieuse procède ainsi à une évaluation *in concreto*.

69. Bien que le défendeur soutienne que les trois services en question font partie de la fonction de deuxième ligne et donc que ces services n'introduisent pas eux-mêmes des traitements, mais se limitent à exercer une surveillance, établir des cadres et réaliser des contrôles, la Chambre Contentieuse vérifie lors de l'audition la relation entre la fonction de deuxième ligne et celle de première ligne afin de savoir si la fonction de deuxième ligne peut assurer sa tâche de conseil et de contrôle sans définir la finalité et les moyens d'éventuels traitements propres et des traitements par la fonction de première ligne. Concrètement, la Chambre Contentieuse constate lors de l'audition que lorsque la fonction de deuxième ligne doit exercer ses compétences de contrôle et de surveillance, elle a également besoin d'informations de la fonction de première ligne. C'est ce qui ressort aussi du registre des activités de traitement dans lequel sont énumérées un nombre important de catégories de données à caractère personnel qui sont traitées par la fonction de deuxième ligne. Selon la Chambre Contentieuse, il en ressort clairement que des données à caractère personnel sont traitées par la fonction de deuxième ligne pour lesquelles elle détermine la finalité et les moyens.

[12] Voir la note de bas de page 11, ci-avant.

70. La réaction du défendeur à cet égard est que la prise de connaissance, à savoir la lecture, de données à caractère personnel n'est pas suffisante pour la qualifier de traitement de données à caractère personnel. Le défendeur fait ainsi une comparaison avec un travailleur qui consulte les données à caractère personnel dans le cadre de son travail, mais n'intervient pas lui-même en tant que responsable distinct du traitement. Suivre une autre interprétation donnerait lieu, selon le défendeur, à ce que chaque travailleur doive être considéré comme responsable distinct du traitement.

71. En ce qui concerne les catégories de données à caractère personnel énoncées dans le registre de traitement qui sont traitées par la fonction de deuxième ligne, le défendeur affirme que celles-ci sont énoncées par 'prudence', parce que la fonction de deuxième ligne peut prendre connaissance de ces données à caractère personnel en vue de l'exercice de ses tâches. Le défendeur y ajoute de nouveau que la fonction de deuxième ligne n'a pas la responsabilité du traitement de données à caractère personnel, mais qu'elle peut prendre connaissance de certaines catégories de données à caractère personnel uniquement de par l'exercice de sa compétence de contrôle et que la fonction de deuxième ligne ne pourra jamais déterminer comment les données à caractère personnel seront interprétées et traitées au sein de la banque.

72. La Chambre Contentieuse fait remarquer que la consultation de données à caractère personnel constitue bel et bien un traitement au sens de l'article 4, 2) du RGPD. Il convient de préciser à cet égard que le traitement de données à caractère personnel n'implique pas que celui qui réalise le traitement, comme par exemple un travailleur, doit être qualifié de responsable distinct du traitement. Le responsable du traitement est celui qui détermine les finalités et les moyens du traitement au sens de l'article 4, 7) du RGPD. La fonction de deuxième ligne participe à la détermination – en tant qu'entité au sein du responsable du traitement – de la finalité et des moyens pour ce qui concerne les données à caractère personnel que la fonction de première ligne doit lui fournir – et participe ainsi en ce sens à la détermination de la finalité et des moyens des traitements du Service de Première Ligne –, afin que la fonction de deuxième ligne puisse assurer sa propre tâche de contrôle et de conseil. Cela ressort indéniablement du registre de traitement. Il en résulte que le délégué à la protection des données, qui revêt également la fonction de chef des services ORM/IRM/SIU, détermine la finalité et les moyens des traitements de données par la fonction de première ligne dans la mesure où cette information est nécessaire pour les tâches dont la fonction de deuxième ligne a été chargée et qu'il définit ensuite également la finalité et les moyens des traitements de données que la fonction de deuxième ligne réalise.

73. Cela mène la Chambre Contentieuse à la conclusion que la combinaison de la qualité de délégué à la protection des données avec la fonction de chef de service des trois services ORM/IRM/SIU n'est pas défendable sans conflit d'intérêts dans le chef du délégué à la protection des données. La Chambre Contentieuse estime dès lors que la **violation de l'article 38.6 du RGPD** est avérée.

74. Il importe que le délégué à la protection des données puisse exécuter ses missions et tâches dans le respect de la position telle que l'article 38 du RGPD la lui a attribuée, en particulier qu'il puisse intervenir sans qu'il y ait conflit d'intérêts. La Chambre Contentieuse charge donc le défendeur de mettre le traitement en conformité avec l'article 38.6 du RGPD sur ce point et ainsi de veiller à ce que ces missions et tâches n'entraînent pas de conflit d'intérêts.

75. Compte tenu du fait que le RGPD a confié un rôle-clé au délégué à la protection des données en lui attribuant une mission informative et consultative à l'égard du responsable du traitement concernant toutes les questions relatives à la protection des données à caractère personnel, dont la notification de violations de données, la Chambre Contentieuse procède également à l'imposition d'une amende administrative.

76. Outre la mesure correctrice visant à mettre le traitement en conformité avec l'article 38.6 du RGPD, la Chambre Contentieuse décide également d'infliger une amende administrative dont le but n'est pas de mettre fin à une infraction commise mais bien de faire appliquer efficacement les règles du RGPD. Comme il ressort du considérant 148, l'idée poursuivie par le RGPD est qu'en cas de violations sérieuses, des sanctions, y compris des amendes administratives, soient infligées, en complément ou à la place des mesures appropriées qui sont imposées.[13] La Chambre Contentieuse agit ainsi en application de l'article 58.2.i) du RGPD. L'instrument de l'amende administrative n'a donc nullement pour but de mettre fin aux violations. À cet effet, le RGPD et la LCA prévoient plusieurs mesures correctrices, dont les ordres cités à l'article 100, § 1er, 8° et 9° de la LCA.

77. Tout d'abord, la nature et la gravité de la violation sont prises en considération par la Chambre Contentieuse afin de justifier l'imposition de cette sanction et l'ampleur de celle-ci.

78. Dans ce cadre, la Chambre Contentieuse constate que bien qu'il n'y ait aucun élément révélant qu'il soit question d'une violation intentionnelle, il s'agit d'un manquement grave dans le chef du défendeur. Bien que le délégué à la protection des données soit une fonction prescrite obligatoirement pour la première fois au niveau européen dans le RGPD, le concept d'un délégué à la protection des données n'est pas nouveau et existe depuis longtemps dans de nombreux États membres et dans de nombreuses organisations.[14]

---

[13] Le considérant 148 dispose ce qui suit : "Afin de renforcer l'application des règles du présent règlement, des sanctions y compris des amendes administratives devraient être infligées pour toute violation du présent règlement, en complément ou à la place des mesures appropriées imposées par l'autorité de contrôle en vertu du présent règlement. En cas de violation mineure ou si l'amende susceptible d'être imposée constitue une charge disproportionnée pour une personne physique, un rappel à l'ordre peut être adressé plutôt qu'une amende. Il convient toutefois de tenir dûment compte de la nature, de la gravité et de la durée de la violation, du caractère intentionnel de la violation et des mesures prises pour atténuer le dommage subi, du degré de responsabilité ou de toute violation pertinente commise précédemment, de la manière dont l'autorité de contrôle a eu connaissance de la violation, du respect des mesures ordonnées à l'encontre du responsable du traitement ou du sous-traitant, de l'application d'un code de conduite, et de toute autre circonstance aggravante ou atténuante. L'application de sanctions y compris d'amendes administratives devrait faire l'objet de garanties procédurales appropriées conformément aux principes généraux du droit de l'Union et de la Charte, y compris le droit à une protection juridictionnelle effective et à une procédure régulière.

[14] Voir notamment WP243Rev01, paragraphe 1.

79. En outre, le Groupe 29 a déjà établi des lignes directrices pour ces délégués le 13 décembre 2016. Ces lignes directrices ont été revues le 5 avril 2017 après une large consultation publique. Comme il ressort de ce qui suit, ces lignes directrices sont claires concernant la mesure dans laquelle le délégué à la protection des données peut également remplir d'autres fonctions au sein de l'entreprise, en tenant compte de la structure organisationnelle propre à chaque organisme, et cet aspect doit être étudié au cas par cas.

80. En bref, selon la Chambre Contentieuse, il n'existe aucun doute quant au fait que le cumul de la fonction de délégué à la protection des données avec une fonction en tant que chef d'un département (au sein duquel des données à caractère personnel sont également traitées) que le délégué à la protection des données doit contrôler ne peut pas avoir lieu de manière indépendante.

81. On peut attendre d'une organisation telle que le défendeur qu'elle se prépare consciencieusement à l'introduction du RGPD et ce dès son entrée en vigueur, conformément à l'article 99 du RGPD en mai 2016. Le traitement de données à caractère personnel constitue en effet une activité centrale du défendeur, qui traite en outre des données à très grande échelle.

82. La durée de l'infraction est également prise en considération. Le délégué à la protection des données a été créé par le RGPD, qui s'applique depuis le 25 mai 2018, de sorte que la violation de l'article 38.6 du RGPD est déjà établie à partir de cette date. En tout état de cause, l'infraction a duré jusqu'à la date de l'entrée en service du délégué à la protection des données engagé à temps plein, c'est-à-dire le 1er juillet 2021.

83. Enfin, le défendeur traite des données à caractère personnel d'un très grand nombre de personnes. Des garanties inefficaces pour la protection des données à caractère personnel, plus précisément en désignant un délégué à la protection des données qui ne répond pas à l'exigence d'indépendance et ne peut donc pas intervenir sans conflit d'intérêts, ont donc un impact potentiel sur un nombre énorme de personnes concernées.

84. L'ensemble des éléments exposés ci-dessus justifie une sanction effective, proportionnée et dissuasive, telle que visée à l'article 83 du RGPD, compte tenu des critères d'appréciation qu'il contient, à concurrence d'un montant de 75.000 euros. La Chambre Contentieuse attire l'attention sur le fait que les autres critères de l'article 83.2 du RGPD ne sont pas, dans ce cas, de nature à conduire à une autre amende administrative que celle définie par la Chambre Contentieuse dans le cadre de la présente décision.

85. Lors de la détermination du montant de l'amende administrative, la Chambre Contentieuse prend en considération les circonstances atténuantes auxquelles le défendeur se réfère dans sa réaction à l'intention de la Chambre Contentieuse d'infliger une amende administrative, à savoir l'absence de dommage pour les personnes concernées (article 83.2 a) du RGPD) ; les mesures prises pour détecter en temps utile et prévenir un potentiel conflit d'intérêts, notamment par la mise en place

de politiques et mécanismes appropriés tels que décrits dans les conclusions (article 83.2, c) du RGPD) ; l'absence de violations pertinentes antérieures (article 83.2 e) du RGPD), ainsi que la collaboration de bonne foi avec l'APD (article 83.2 f) du RGPD).

86. Pour répondre concrètement à l'objection du défendeur, la Chambre Contentieuse affirme qu'il n'a certes pas été constaté qu'il était question de dommage dans le chef des personnes concernées, mais l'absence de tout dommage n'a pas non plus été démontrée, et des violations n'ont pas été constatées antérieurement. Ce constat a amené la Chambre Contentieuse à ramener le montant initialement envisagé de l'amende administrative, à savoir 100.000 EUR, à 75.000 EUR.

87. En ce qui concerne la mise en œuvre de politiques et mécanismes destinés à éviter les conflits d'intérêts, la Chambre Contentieuse fait remarquer que ceux-ci ont été pris tardivement, c'est-à-dire bien après l'entrée en vigueur[15] et l'application[16] du RGPD. La 'Conflicts of Interest Policy' date du 20 janvier 2020 et la politique spécifique au DPO a été mise en œuvre le 12 octobre 2020 suite à la décision quant au fond n° 18/2020 du 28 avril 2020, comme indiqué dans les conclusions, et un délégué à la protection des données à temps plein n'a été désigné que le 1er juillet 2021. Cela signifie que le défendeur a certes collaboré avec l'APD pour remédier à la violation et en limiter les éventuels effets négatifs, mais cela s'est produit bien après l'entrée en vigueur et la mise en application du RGPD, ce qui a un impact sur la durée de la violation (voir le point 82 ci-avant).

88. En ce qui concerne le montant de l'amende, le défendeur objecte que l'amende est plus élevée que celle infligée pour une violation identique dans la décision quant au fond n° 18/2020 du 28 avril 2020, alors que le défendeur affirme que son chiffre d'affaires consolidé est inférieur, qu'il a déjà pris des mesures pour répondre aux préoccupations de l'APD et qu'il a une position moindre sur le marché.

89. La Chambre Contentieuse déclare que le montant maximal de l'amende administrative pour une violation de l'article 38 du RGPD est définie à l'article 83.4 du RGPD[17]. Le montant de l'amende infligée dans la présente décision est sensiblement inférieur au montant maximal défini à l'article 83.4 du RGPD, étant donné que la Chambre Contentieuse a pris en considération l'ensemble des critères repris à l'article 83.2 du RGPD. En outre, la Chambre Contentieuse évalue les éléments concrets de chaque dossier de manière distincte afin d'infliger une sanction appropriée[18].

---

[15] En vertu de l'article 99.1 du RGPD, le RGPD est entré en vigueur le 25 mai 2016.

[16] L'article 99.2 du RGPD dispose que le RGPD est applicable à compter du 25 mai 2018.

[17] Article 83.4 du RGPD. *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 ;

[…]

[18] Voir à cet égard l'arrêt de la Cour des marchés du 7 juillet 2021, numéro de rôle 2021/AR/320, NV Nationale Dienst voor Promotie van Kinderartikelen (N.D.P.K. N.V.) c. APD, p. 42

La référence du défendeur à la décision quant au fond n° 18/2020 du 28 avril 2020 concerne la même violation, à savoir l'existence d'un conflit d'intérêts dans le chef du délégué à la protection des données (article 38.6 du RGPD) mais pour le reste, la Chambre Contentieuse doit tenir compte de tous les éléments de fait propres à chaque dossier distinct. Dans le présent dossier, la durée de la violation constitue un élément important, ce qui justifie en l'espèce une amende de 75.000 EUR, pour laquelle la Chambre Contentieuse se base sur les comptes annuels consolidés du défendeur.

d) Registre des activités de traitement (article 30 du RGPD)

90. En ce qui concerne le registre des activités de traitement, le Service d'Inspection fait les constats suivants, tels que résumés ci-après :

- le registre des activités de traitement des services ORM/IRM/SIU[19] est incomplet ;
- le registre des activités de traitement ne comporte que trois activités de traitement, à savoir une seule activité de traitement pour chacun des services. Le Service d'Inspection trouve cela étrange, étant donné que dans chacun des trois services, il y a différentes activités de traitement au sein de la fonction de deuxième ligne et il est donc plutôt anormal de reprendre ces activités de traitement sous une seule activité de traitement ;
- le défendeur n'a pas prévu une énumération complète de toutes les finalités de traitement des données à caractère personnel, conformément à l'article 30.1 b) du RGPD ;
- les informations suivantes du registre des activités de traitement ne sont pas visibles :
    - le nom et les coordonnées du délégué à la protection des données, conformément à l'article 30.1 a) du RGPD ;
    - une description des délais envisagés dans lesquels les différentes catégories de données doivent être effacées, conformément à l'article 30.1 f) du RGPD ;
    - une description des mesures de sécurité techniques et organisationnelles, conformément à l'article 30.1 g) du RGPD.
- le registre des activités de traitement proprement dit doit être complet et clair, mais les termes suivants ne sont pas expliqués : *"12. TIN" et "S9. Criminal data"*. La description des finalités du traitement est vague également : "*E7_To support the activities to safeguard and ensure the security and integrity of Y and/or the financial sector*" et *"C6_Compliance with legal obligations*", et ne restitue pas précisément l'activité de traitement et la finalité du traitement de ces services du défendeur.

[19] Operational Risk Management (ORM)/Information Risk Management (IRM)/Special Investigation Unit (SIU).

- spécifiquement pour le service SIU, le registre des activités de traitement mentionne que les données à caractère personnel concernant des condamnations pénales et des infractions sont traitées avec la mention suivante "*S9. Criminal data*". Le Service d'Inspection trouve étrange que cela ne soit pas expliqué spécifiquement.

91. Le défendeur fait valoir ce qui suit au sujet de ces constatations du Service d'Inspection :

- Excepté l'énumération des éléments qui doivent obligatoirement être repris dans le registre et l'obligation de communiquer le registre à l'autorité de contrôle sur demande, le RGPD n'impose aucune autre obligation légale concernant le registre. Selon le défendeur, le Service d'Inspection semble donc, par ses constatations dans le rapport d'inspection, vouloir placer la barre plus haut que les exigences légales en la matière. Le défendeur ajoute et démontre qu'il a en outre tenu compte de la recommandation n° 06/2017 du 14 juin 2017, telle que formulée par la Commission de la protection de la vie privée ;

- En ce qui concerne les termes vagues et la description vague des finalités du traitement, le défendeur affirme que le registre est un instrument interne et une aide pour le responsable du traitement. Le défendeur reconnaît que le registre sert également de source d'information pour l'APD et qu'en ce sens, il doit également être compréhensible pour l'APD elle-même. Il n'est toutefois pas exclu que le responsable du traitement puisse encore donner des explications à l'APD pour certaines terminologies internes utilisées dans le registre. L'article 30.1 du RGPD requiert que le registre des activités de traitement comporte une description des catégories de données à caractère personnel, ainsi que des finalités de traitement, mais ne comporte pas d'obligation concrète quant au niveau de détail de ces catégories de données à caractère personnel et des finalités de traitement. Dans la recommandation précitée n° 06/2017, on donne d'ailleurs des exemples de catégories de données à caractère personnel et de finalités qui sont de même nature "générale".

  En ce qui concerne les notions et finalités que le Service d'Inspection qualifie de vagues, le défendeur affirme que celles-ci ont été définies dans un autre document interne. Les définitions de ce document – tant en ce qui concerne les catégories de données à caractère personnel que les finalités – ont été reprises dans le registre et étaient déjà disponibles dans le registre en cliquant sur les termes en question.

- Le défendeur souligne que le Service d'Inspection n'a réclamé que le registre des activités de traitement des services ORM/IRM/SIU et non le registre complet. Le document fourni par le défendeur était un extrait limité du registre et comprend uniquement les détails des activités de traitement des services concernés.

- Les activités de traitement des services ORM, IRM et SIU sont expliquées davantage par le défendeur. Il déclare que les services IRM et ORM ont principalement une nature d'avis et de

contrôle, sans avoir réellement de tâche d'exécution au niveau du traitement d'informations et/ou de données à caractère personnel. Il s'agit de traitements très limités qui sont groupés dans le registre sous une seule activité de traitement pour chacun des deux services. Un certain nombre d'activités de traitement que le Service d'Inspection attribue respectivement au service IRM et au service ORM sont des activités qui sont décrites ailleurs dans le registre pour les sections qui en sont responsables. En ce qui concerne le service SIU, les activités sont également décrites et ici aussi, elles ont été reprises de manière groupée dans l'extrait du registre comme une seule activité de traitement. Le défendeur souligne de nouveau que le RGPD ne prévoit aucun niveau de détail spécifique requis.

- En ce qui concerne les informations qui, selon le rapport d'inspection, sont manquantes dans le registre des activités de traitement, le défendeur avance que le nom et les coordonnées du délégué à la protection des données sont repris dans un grand nombre de documents internes et sont donc bien connus au sein de l'organisation du défendeur, mais que ces données concernant le délégué à la protection des données n'apparaissent pas dans l'extrait du registre des activités de traitement pour des raisons purement techniques.

  En ce qui concerne les délais de conservation, ainsi que les mesures techniques et organisationnelles, l'article 30 du RGPD prescrit que le registre contient ces informations *dans la mesure du possible*, mais n'impose pas en tant que tel de les mentionner dans le registre proprement dit. Le défendeur affirme qu'il a été décidé de décrire ces informations dans des documents distincts pour des raisons pragmatiques et en vue d'une meilleure clarté.

92. Sur la base de la défense et des pièces justificatives, la Chambre Contentieuse décide que dans le chef du défendeur, **il n'y a pas de violation de l'article 30 du RGPD**.

III. Publication de la décision

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

PAR CES MOTIFS,

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

- en vertu de l'article 100, § 1er, 5° de la LCA, d'ordonner un non-lieu pour la violation des articles 5.1 d), 16 et 25 du RGPD ;
- en vertu de l'article 100, § 1er, 13° et de l'article 101 de la LCA, d'infliger une amende administrative de 75.000 € suite à la violation de l'article 38.6 du RGPD.

En vertu de l'article 108, § 1er de la LCA, cette décision peut faire l'objet d'un recours auprès de la Cour des marchés dans un délai de trente jours à compter de sa notification, avec l'Autorité de protection des données en qualité de défenderesse.

(sé.) Hielke Hijmans

Président de la Chambre Contentieuse