Chambre Contentieuse

Décision quant au fond 56/2021 du 26 avril 2021

N° de dossier : DOS-2019-02288

Objet : Plainte pour consultation illicite des données personnelles et refus de droit d'accès

La Chambre Contentieuse de l'Autorité de protection des données, constituée de Monsieur Hielke Hijmans, président, et de Messieurs Yves Poullet et Christophe Boeraeve, membres, reprenant l'affaire en cette composition ;

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 : Mme X, représentée par son conseil Maître Victor Rouard, Avenue des arts 46, à 1000 Bruxelles,

- La défenderesse : La Y, représentée par ses conseils, Maître Didier Putzeys et Me Bernadette De Graeuwe, avenue Brigade Piron 132 à 1080 Bruxelles.

1. **Rétroactes de la procédure**

1. Vu la première plainte déposée le 15 avril 2019 par la plaignante à l'Autorité de protection des données (APD), suivie d'une seconde plainte déposée le 20 avril 2020 ;

2. Vu la décision du 21 avril 2020 du Service de première ligne de l'Autorité de protection des données (ci-après « APD ») déclarant la plainte recevable et la transmission de celle-ci à la Chambre Contentieuse à cette même date ;

   Vu la communication du 31 juillet 2020 de la Chambre Contentieuse informant les parties de sa décision de considérer le dossier comme étant prêt pour traitement au fond sur la base de l'article 98 LCA, et l'envoi du calendrier d'échange de conclusions ;

3. Vu les conclusions de la défenderesse, reçues le 8 septembre 2020 ;

4. Vu les conclusions du plaignant, reçues le 30 septembre 2020 ;

5. Vu les conclusions de synthèse de la défenderesse, reçues le 21 octobre 2020.

6. Vu l'audition du 07 janvier 2021 en présence de la plaignante, son conseil Me Rouard, ainsi que la défenderesse représentée par son conseil Me De Graeuwe, de même que la DPO, Mme Z1 , et le Compliance Officer, M.Z2 ;

7. Vu l'envoi aux parties du PV d'audition et les commentaires des parties ;

8. Vu la disjonction des procédures contre l'ex-mari de la plaignante et contre la défenderesse ;

9. Vu le formulaire d'amende envoyé à la partie défenderesse et ses observations.

2. **Les faits et l'objet de la plainte**

10. La plaignante apprend en avril 2019 que vingt consultations ont été faites de ses données à caractère personnel hébergées dans son fichier à la Centrale des Crédits aux Particuliers (ci-après CCP) à la Banque Nationale Belge (ci-après BNB) par la défenderesse entre 2016 et 2018.

11. La défenderesse est active dans le secteur des services financiers, dont les crédits aux particuliers. L'ex-époux de la plaignante, avec lequel elle était en instance de sortie d'indivision suite à leur divorce depuis 2015, est employé par la défenderesse. La plaignante avance qu'en consultant ses

données dans son fichier à la BNB et ainsi les informations relatives à ses crédits, son ex-mari a pris l'ascendant dans l'indivision et lui aurait causé un préjudice financier et moral.

12. L'ex-mari de la plaignante a par ailleurs reconnu avoir consulté abusivement les données de celle-ci[1].

13. Le 14 novembre 2018 la plaignante s'adresse à la BNB afin de demander la liste des organismes financiers qui ont consulté le fichier de la CCP à son nom.

14. Le 24 janvier 2019 la plaignante s'adresse à la défenderesse afin de demander « *quels sont vos critères pour consulter les fichiers de la Banque Nationale de vos clients et savoir si Y ou toute autre personne est autorisé à les consulter sans demande spécifique de financement.* »

15. Le 1 février 2019, l'ancien Data Protection Officer (DPO) de la défenderesse, lui répond que les fichiers de la CCP *«sont uniquement consultés dans le cadre de l'octroi ou de la gestion de crédits ou de services de paiement, susceptibles de grever le patrimoine privé d'une personne physique et dont l'exécution peut être poursuivi* (sic) *sur le patrimoine privé de cette personne.* ».

16. Or, la plaignante explique n'avoir aucun dossier de crédit ouvert chez la défenderesse. Lors de l'audition du 7 janvier 2021, la DPO de la défenderesse a confirmé que la plaignante n'a pas de dossier en cours, mais bien un dossier clôturé chez elle, ce qui explique d'un point de vue technique que l'ex-époux ait pu accéder au fichier CCP.

17. Le 13 mars 2019 la plaignante demande quelles sont les sanctions encourues par un employé qui ne respecte pas les règles en matière de protection des données. Le DPO répond le 21 mars 2019 en demandant un complément d'informations. Il propose un entretien téléphonique afin de faciliter la communication.

18. La plaignante répond en acceptant mais en précisant que *« c'est très délicat, car dans un premier temps je n'ai pas envie de porter préjudice à qui que ce soit même si j'ai des preuves officielles »*. L'entretien téléphonique entre la nouvelle DPO de la défenderesse et la plaignante a bien eu lieu.

19. Dans un mail du 5 avril 2019 la plaignante fait état du détail des consultations de son fichier à la CCP, reçu de la BNB le 14 novembre 2018, qui porte sur une période allant d'avril 2016 à août 2018.

[1] cf conclusions additionnelles et de synthèse de la défenderesse p14

20. Elle joint ce document à son mail. Dans ce mail, elle accuse son ex-mari d'être l'auteur des 20 consultations par la défenderesse de son fichier à la CCP depuis 2016.

21. Elle ne demande pas confirmation de ses allégations mais avant de déposer plainte contre son ex-mari, elle demande les sanctions encourues par celui-ci pour avoir commis cette intrusion dans sa vie privée.

22. Le 11 avril 2019, la nouvelle DPO de la défenderesse

    - répond qu'elle ne dispose pas des éléments lui permettant de justifier toutes les consultations reprises dans la liste fournie par la BNB,

    - confirme les règles de consultation du registre de la BNB applicables aux employés de la défenderesse,

    - confirme l'existence de mesures disciplinaires à l'encontre des employés ne respectant pas ces règles, et

    - refuse de répondre aux questions de la plaignante sur la nature de la sanction infligée à son ex-mari, au titre de la vie privée des employés de la SA.

23. Le 15 avril 2019, la plaignante introduit une première plainte auprès de l'APD pour consultations illicites de ses données à la BNB par son ex-mari, via ses fonctions chez la défenderesse, et demande à être informée des sanctions encourues par son ex-mari.

24. Le 5 septembre 2019 le Service de Première Ligne (« SPL ») de l'APD prend contact avec la défenderesse pour l'avertir qu'elle avait été saisie d'une plainte par la plaignante et demandant la base légale et la justification de la consultation à 20 reprises, par la défenderesse, des données de la plaignante dans la banque de données de la BNB. Elle lui demande également de communiquer à la plaignante la liste de toutes les consultations de la base de données de la CCP, l'identité des personnes ayant consulté, ainsi que les données consultées.

25. Le 13 septembre 2019 la défenderesse répond à l'APD :
    - qu'elle n'a jamais approuvé, ni toléré la consultation faite par l'un de ses employés, des données relatives à la plaignante se trouvant dans la CCP ;

    - que toute consultation faite en dehors du cadre de la conclusion d'un contrat de crédit à la consommation ou de la gestion de celui-ci est interdite ;

- que des mesures de contrôle et une procédure disciplinaire existent pour éviter et sanctionner de tels agissements et que l'auteur de ces consultations illicites a été sanctionné ;

- qu'elle ne peut pas donner de base légale, ces consultations ayant été faites en dehors des procédures normales, elle ne peut pas non plus indiquer les noms des personnes ayant consulté, ni les données consultées, ni communiquer la liste de ces consultations car le système informatique ne permet pas de garder des traces du traitement tel qu'effectué par l'ex-mari de la plaignante En effet, l'ex-mari de la plaignante, en sa qualité de cadre, dispose d'un accès différent de celui des employés non cadres (« collaborateurs ») au registre de la BNB. Les spécificités techniques de ce système d'accès empêchent, selon la défenderesse, la conservation de toute trace des consultations qu'il a faites[2].

26. Le 21 octobre 2019 le SPL répond qu'il revient au responsable du traitement d'assurer la sécurité et la confidentialité des données qu'il collecte et doit répondre à la demande d'accès conformément à l'article 15 RGPD. La plaignante a dès lors le droit d'obtenir la liste des données qui ont été consultées, l'identité des personnes ayant consulté, la finalité et la base légale. Ces informations ne sont pas transmises à la plaignante.

27. Le 20 avril 2020 la plaignante dépose une nouvelle plainte à l'APD contre son ex-mari et contre la défenderesse pour consultation abusive de ses fichiers personnels auprès de la BNB via les fonctions de son ex-mari au sein de la défenderesse. Elle demande aussi à ce que son ex-mari soit sanctionné de manière adéquate et être informée de cette sanction.

28. Suite à la disjonction des procédures, les parties ont été informées que le volet de la plainte relatif à l'ex-mari de la plaignante sera examiné dans un dossier séparé. La présente décision couvre uniquement le volet de la plainte relatif à la défenderesse.

29. L'analyse juridique de la plainte - corroborée par les conclusions déposées par la plaignante - indique que celle-ci soulève :
-la violation des principes de finalité, loyauté, transparence, et information (articles 5,12,13,14 RGPD) ;
- la violation des obligations de sécurité (article 32, combiné aux articles 5.2 et 24 du RGPD

[2] Voy conclusions additionnelles et de synthèse de la défenderesse, p.18

- l'absence d'indépendance du DPO (article 38 RGPD) ;
- l'absence de facilitation par Y dans l'exercice par la demanderesse de ses droits et violation de son droit d'accès.

30. La plaignante invite dans ses conclusions la Chambre Contentieuse à :

- ordonner à la défenderesse de lui transmettre un relevé de l'ensemble des consultations de ses données par la défenderesse (avec la date, identité de la personne ayant consulté, licéité ou non de la consultation) ;
- ordonner à la défenderesse de mettre en conformité le traitement des données consultées dans le cadre de ses activités et lui faire parvenir les mesures correctives instaurées afin d'assurer la sécurisation des traitements ;
- imposer une amende à la défenderesse en tenant compte de la gravité des violations, de sa durée, du nombre de personnes concernées, et de l'attitude de la défenderesse.

31. La défenderesse réfute les griefs.

3- Quant aux motifs de la décision

I- Sur la compétence de l'APD

32. En application de l'article 4.1 LCA, l'APD est responsable du contrôle des principes de la protection des données, tels qu'affirmés par le RGPD et d'autres lois contenant des dispositions relatives à la protection du traitement des données à caractère personnel.

33. En application de l'article 33.1 LCA, la Chambre Contentieuse est l'organe de contentieux administratif de l'APD[3]. Elle est saisie des plaintes que le SPL lui transmet en application de l'article 62.1 LCA, soit des plaintes recevables dès lors que conformément à l'article 60 alinéa 2 LCA, ces plaintes sont rédigées dans l'une des langues nationales, contiennent un exposé des faits et les indications nécessaires pour identifier le traitement de données à caractère personnel sur lequel elles portent et relèvent de la compétence de l'APD.

34. En application des articles 51 et s. du RGPD et de l'article 4.1 LCA, il revient à la Chambre Contentieuse en tant qu'organe de contentieux administratif de l'APD, d'exercer un contrôle effectif de l'application du RGPD et de protéger les libertés et droits fondamentaux des personnes

[3] La nature administrative du contentieux devant la Chambre Contentieuse a été confirmée par la Cour des marchés, juridiction d'appel des décisions de la Chambre Contentieuse. Voy. notamment l'arrêt du 12 juin 2019, publié sur le site de l'APD ,ainsi que la décision 17/2020 de la Chambre Contentieuse.

physiques à l'égard du traitement et de faciliter le libre flux des données à caractère personnel au sein de l'Union.

35. Comme la Chambre Contentieuse a déjà eu l'occasion de l'énoncer[4], des traitements de données sont opérés dans de multiples secteurs d'activité, notamment dans le cadre professionnel comme dans le cas d'espèce. Il n'en demeure pas moins que la compétence de l'APD en général, et de la Chambre Contentieuse en particulier, est limitée au contrôle du respect de la règlementation applicable aux traitements de données, quel que soit le secteur d'activité dans lequel ces traitements de données interviennent. Son rôle n'est pas de se substituer aux juridictions de l'ordre judiciaire dans l'exercice des compétences qui sont les leurs. Dès lors, comme la défenderesse relève par ailleurs dans ses conclusions, la Chambre Contentieuse n'est pas compétente pour se prononcer sur la teneur de la sanction disciplinaire imposée par la défenderesse à l'ex-époux de la plaignante, suite aux consultations illicites qu'il a opérées. Néanmoins, conformément à l'article 51 RGPD, l'APD demeure compétente pour vérifier l'effectivité des mesures organisationnelles mises en place en cas de violation des dispositions du RGPD, notamment celles relatives à la sécurité des traitements. Dans cette mesure, l'APD se réserve le droit d'obtenir la communication par la défenderesse de la nature de la sanction disciplinaire imposée à l'ex-mari de la plaignante, ainsi que toute autre mesure mise en place pour éviter de nouveaux traitements illicites par les employés de la défenderesse.

36. Comme indiqué supra, suite à la décision de la Chambre Contentieuse de disjoindre les procédures, la présente décision n'examine pas le volet de la plainte relatif à l'ex-mari de la plaignante, mais uniquement le volet relatif à la défenderesse. Dans la mesure où la défenderesse est active dans le secteur bancaire et traite des volumes importants de données financières sensibles, et prenant en considération qu'elle fait partie d'une multinationale occupant plus de 10.000 employés en Belgique , ainsi qu'au vu du fait que l'exercice effectif des droits des personnes concernées (dont le droit d'accès) fait partie des priorités thématiques de l'APD[5], la Chambre Contentieuse estime opportun d'examiner par priorité ce volet de la plainte.

37. La Chambre relève aussi que le conflit entre la plaignante et son ex-mari est lié au divorce entre eux et à leur sortie d'indivision, aspects qui ne relèvent pas du droit à la protection des données.

38. Pour le surplus, la Chambre Contentieuse note que si elle n'est pas compétente pour les consultations illicites ayant eu lieu avant le 25 mai 2018, date d'entrée en vigueur du RGPD, elle l'est bien pour les consultations ultérieures. Dans la mesure où les consultations se sont étendues jusqu'en août 2018, la Chambre Contentieuse est bien compétente.

---

[4] Voy. notamment la décision 03/2020 de la Chambre Contentieuse.

[5] Voir les priorités 2019-2025 de l'APD dans son Plan stratégique, publié sur le site.

II- Sur le fond

II.1- Quant à la qualité de responsable du traitement et de sous-traitant

II.1.1- Définitions et qualité de responsable du traitement et de sous-traitant

39. Conformément à l'article 4.7 du RGPD, il y a lieu de considérer comme le 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. »

40. L'article 4.8 du RGPD stipule qu'il y a lieu de considérer comme le sous-traitant : « la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement. »

41. L'Autorité de Protection des Données a par ailleurs spécifié les aspects suivants sur la qualité de sous-traitant :« L'existence de la sous-traitance dépend du responsable de traitement qui doit avoir décidé de ne pas réaliser lui-même le traitement dont il maitrise la ou les finalités et/ou moyens mais d'en déléguer tout ou une partie des opérations à une autre personne ou organisation extérieure que la sienne. Cette autre personne doit être juridiquement distincte de l'organisation du responsable de traitement et doit réaliser les opérations de traitement de données à caractère personnel déléguées pour le compte de ce dernier et conformément à ses instructions documentées. »[6] (nous soulignons).

42. Conformément aux Lignes directrices 07/2020 de l'EDPB[7], la Chambre Contentieuse évalue concrètement le rôle et la qualité du (des) responsable(s) du traitement concerné(s).

43. 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 de la CCP de la BNB sont effectuées uniquement dans le cadre de l'octroi de crédit aux particuliers ou dans la gestion de ces dossiers. C'est par ailleurs la défenderesse qui met à disposition les moyens pour effectuer ce traitement (via ses systèmes informatiques). Elle doit donc être considérée comme un responsable de traitement.

---

[6] Note de l'APD "Le point sur les notions de responsable de traitement / sous-traitant au regard du Règlement (UE) n° 2016/679 du Parlement européen et du Conseil du 27 avril 2016 sur la protection des données à caractère personnel (RGPD) et quelques applications spécifiques aux professions libérales telles que les avocats", septembre 2018, p 2.

[7] EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 02 September 2020, point 12.

44. Il convient néanmoins de souligner d'emblée 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 (…)»[8]. Que la défenderesse soit responsable de traitement pour les consultations de ses employés au registre CCP 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 CCP dans le cadre des finalités de la défenderesse (octroi ou gestion de crédits), des consultations abusives opérées à des fins privées par l'ex-mari de la plaignante. Comme il est indiqué ci-dessous, bien qu'il ait utilisé les moyens mis à sa disposition par la défenderesse, dans la mesure où l'ex-mari de la défenderesse a opéré les consultations litigieuses en dehors du cadre de ses tâches en tant qu'employé de la défenderesse, il doit être considéré comme responsable de traitement pour ces consultations abusives spécifiquement.

45. Comme l'indique l'EDPB, ceci n'exempte néanmoins en rien la défenderesse, en tant que responsable du traitement, des consultations au registre de la CCP, de son obligation d'assurer la sécurité des traitements[9]. Cet aspect est développé infra (voir II.1.2- Sur la responsabilité du responsable de traitement).

46. En ce qui concerne la qualité de sous-traitant, la Chambre Contentieuse estime que la plaignante ne peut être suivie dans son argumentation selon laquelle l'ex-mari de la plaignante est sous-traitant de la défenderesse. En effet, les deux conditions mentionnées supra ne sont pas remplies. L'ex-mari de la plaignante, en tant qu'employé, n'est pas une entité juridique distincte de la défenderesse, et il n' a pas effectué le traitement pour le compte et sur base des instructions de la défenderesse.

47. Dès lors, le grief du non-respect des obligations relatives à la sous-traitance (article 28 RGPD) tel que développé par la plaignante est non pertinent, et n'est pas examiné plus avant dans le cadre de cette décision.

II.1.2- Sur la responsabilité du responsable de traitement

[8] CJUE, aff. C-210/16, 5 juin 2018, ECLI:EU:C:2018:388, §29.

[9] Avis 1/2010 sur les notions de «responsable du traitement» et de «sous-traitant», WP169, p.17.

48. La défenderesse se réfère à l'avis 1/2010 du Groupe 29 sur les notions de « responsable du traitement » et de « sous-traitant »[10], pour affirmer qu'elle n'est pas responsable de traitement et que cette qualité doit être reconnue dans le chef de l'ex-mari de la plaignante.

49. La Chambre souligne les passages suivants de cet avis (p16-19) :

« Dans la perspective stratégique d'attribution des responsabilités, et afin que les personnes concernées puissent s'adresser à une entité plus stable et plus fiable lorsqu'elles exercent les droits qui leurs sont conférés par la directive, il serait préférable de considérer comme responsable du traitement la société ou l'organisme en tant que tel, plutôt qu'une personne en son sein. C'est en effet la société ou l'organisme qu'il convient de considérer, en dernier ressort, comme responsable du traitement des données et des obligations énoncées par la législation relative à la protection des données, à moins que certains éléments précis n'indiquent qu'une personne physique doit être responsable.

D'une manière générale, on partira du principe qu'une société ou un organisme public est responsable en tant que tel des opérations de traitement qui se déroulent dans son domaine d'activités et de risques.

50. Parfois, les sociétés et les organismes publics désignent une personne précise pour être responsable de l'exécution des opérations de traitement. Cependant, même lorsqu'une personne physique est désignée pour veiller au respect des principes de protection des données ou pour traiter des données à caractère personnel, elle n'est pas responsable du traitement mais agit pour le compte de la personne morale (société ou organisme public), qui demeure responsable en cas de violation des principes, en sa qualité de responsable du traitement. » (nous soulignons)

51. La défenderesse se réfère plus spécifiquement au paragraphe suivant de l'avis :

« Une analyse distincte s'impose dans le cas où une personne physique agissant au sein d'une personne morale utilise des données à des fins personnelles, en dehors du cadre et de l'éventuel contrôle des activités de la personne morale. Dans ce cas, la personne physique en cause serait responsable du traitement décidé, et assumerait la responsabilité de cette utilisation de données à caractère personnel. Le responsable du traitement initial pourrait néanmoins conserver une certaine part de responsabilité si le nouveau traitement a eu lieu du fait d'une insuffisance des mesures de sécurité. »

[10] Avis 1/2010 sur les notions de «responsable du traitement» et de «sous-traitant», WP169, p.17.

52. La Chambre Contentieuse souligne la partie suivante du même avis :

« Pour résumer les réflexions qui viennent d'être exposées, il apparaît que la personne responsable en cas de non-respect de la protection des données est toujours le responsable du traitement, à savoir la personne morale (société ou organisme public) ou la personne physique formellement identifiée selon les critères de la directive. Si une personne physique travaillant dans une société ou un organisme public utilise des données à des fins personnelles, en dehors des activités de la société, elle doit être considérée comme un responsable du traitement de fait et assumer la responsabilité pénale en tant que tel. » (p18) (nous soulignons)

53. Le Groupe de Travail cite de même un exemple :

« Exemple n° 4: Surveillance secrète des employés

Un membre du conseil d'administration d'une société décide de surveiller secrètement les employés de la société, alors que cette décision n'a pas officiellement reçu l'aval du conseil d'administration. La société doit être considérée comme responsable du traitement et faire face aux éventuelles réclamations et poursuites des employés dont les données à caractère personnel ont été utilisées abusivement.

> La responsabilité juridique de la société est notamment due au fait qu'en tant que responsable du traitement, elle a l'obligation de garantir le respect des règles de sécurité et de confidentialité. Une utilisation abusive par un dirigeant de la société ou un employé pourrait être considérée comme le résultat de mesures de sécurité inappropriées.

Il importe à cet égard que le membre du conseil d'administration ou d'autres personnes physiques dans la société soient ultérieurement tenues pour responsables, tant en matière civile (également envers la société) que pénale. Cela pourrait notamment être le cas si le membre du conseil s'est servi des données collectées pour obtenir des faveurs personnelles des employés: il devrait alors être considéré comme «responsable du traitement» et voir sa responsabilité engagée pour cette utilisation des données. » (p18-19)

54. Cet avis 1/2010 a été remplacé par des Lignes directrices 07/2020 de l'EDPB (successeur du Groupe 29), selon lesquelles :

"Whereas the terms "personal data", "data subject", "controller" and "processor" are defined in the Regulation, the concept of "persons who, under the direct authority of the controller or processor, are authorised to process personal data" is not. It is, however, generally understood

as referring to persons that belong to the legal entity of the controller or processor (an employee or a role highly comparable to that of employees, e.g. interim staff provided via a temporary employment agency) but only insofar as they are authorized to process personal data."[11]

(traduction libre:

55. Alors que les termes "données à caractère personnel", "personne concernée", "responsable du traitement" et "sous-traitant" sont définis dans le règlement, la notion de "personnes qui, sous l'autorité directe du responsable du traitement ou du sous-traitant, sont autorisées à traiter des données à caractère personnel" ne l'est pas. Ce concept est toutefois généralement entendu comme faisant référence aux personnes qui appartiennent à l'entité juridique du responsable du traitement ou du sous-traitant (un employé ou un rôle hautement comparable à celui des employés, par exemple le personnel intérimaire fourni par l'intermédiaire d'une agence de travail temporaire) mais uniquement dans la mesure où elles sont autorisées à traiter des données à caractère personnel".)

56. Une lecture attentive de l'avis montre qu'à l'inverse, un employé n'ayant pas accès dans le cadre de ses fonctions à des données à caractère personnel, qu'il utiliserait à ses propres fins, doit être considéré comme une tierce partie, c'est-à-dire comme une entité distincte de son employeur :

57. « An employee etc. who obtains access to data that he or she is not authorised to access and for other purposes than that of the employer does not fall within this category. Instead, this employee should be considered as a third party vis-à-vis the processing undertaken by the employer. Insofar as the employee processes personal data for his or her own purposes, distinct from those of his or her employer, he or she will then be considered a controller and take on all the resulting consequences and liabilities in terms of personal data processing".[12]

(traduction libre:

58. Un employé, etc. qui obtient l'accès à des données auxquelles il n'est pas autorisé à accéder et à des finalités autres que celles de l'employeur n'entre pas dans cette catégorie. Cet employé doit plutôt être considéré comme un tiers vis-à-vis du traitement effectué par l'employeur. Dans la mesure où l'employé traite des données à caractère personnel pour ses propres finalités, distinctes de celles de son employeur, il sera alors considéré comme responsable du traitement et assumera toutes les conséquences et responsabilités qui en découlent en termes de traitement des données à caractère personnel.)

[11] Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 2 September 2020, point 86, p27
[12] Ibid .

59. Dans le cas d'espèce, bien que l'ex-mari de la plaignante avait accès à la CCP sur base de sa mission de contrôle des dossiers de crédit, les consultations litigieuses ont été opérées en dehors du cadre de ses tâches en tant qu'employé. Il convient de suivre le raisonnement adopté par l'EDPB dans les Lignes directrices 07/2020, et par conséquent de considérer l'ex-mari comme tierce partie distincte de la défenderesse pour les consultations abusives spécifiquement.

60. La défenderesse doit donc être suivie dans son argument selon lequel l'ex-mari est responsable de traitement pour les consultations abusives.

61. La Chambre relève néanmoins que la responsabilité de l'ex-mari n'est pas examinée dans la présente décision, mais uniquement celle de la défenderesse, dans la mesure où les procédures envers ces deux parties ont été disjointes.

62. La Chambre distingue donc les traitements opérés dans le cadre des consultations du registre CCP telles que prévues par les finalités de la défenderesse, des consultations abusives opérées par l'ex-époux de la plaignante. Bien que celui-ci soit responsable de traitement pour les consultations abusives, la défenderesse reste responsable de traitement pour les consultations au registre CCP dans le cadre des finalités qu'elle détermine (octroi ou gestion des crédits des particuliers). Dans ce cadre, elle reste soumise au principe de responsabilité (articles 5.2 et 24 RGPD) en tant que responsable de traitement et employeur, ainsi qu'aux articles 29 RGPD[13] et 32 RGPD, en particulier en son paragraphe 4[14].

63. Dans la mesure où il revient au responsable de traitement de garantir la sécurité des traitements (y compris l'accès aux données en conformité avec le GDPR par ses employés), il revenait à la défenderesse d'implémenter les mesures techniques et organisationnelles appropriées pour éviter des traitements abusifs par ses employés, comme en l'espèce (cet aspect est développé infra). Ceci est d'autant plus d'application au vu de la nature sensible des données auxquelles les employés de la défenderesse ont accès (données financières). Cette position est aussi celle défendue dans la doctrine[15].

---

[13] Article 29 RGPD : « *Le sous-traitant et toute personne agissant sous l'autorité du responsable du traitement ou sous celle du sous-traitant, qui a accès à des données à caractère personnel, ne peut pas traiter ces données, excepté sur instruction du responsable du traitement, à moins d'y être obligé par le droit de l'Union ou le droit d'un État membre* »

[14] Article 32.4 RGPD : « *Le responsable du traitement et le sous-traitant prennent des mesures afin de garantir que toute personne physique agissant sous l'autorité du responsable du traitement ou sous celle du sous-traitant, qui a accès à des données à caractère personnel, ne les traite pas, excepté sur instruction du responsable du traitement, à moins d'y être obligée par le droit de l'Union ou le droit d'un État membre.* »

[15] Delforge, A., « Titre 8 - Les obligations générales du responsable du traitement et la place du sous-traitant » in Le règlement général sur la protection des données (RGPD/GDPR), Bruxelles, Éditions Larcier, 2018, p. 374

64. Si à l'inverse, et comme l'avance la partie défenderesse, l'employeur devait être exempté de toute responsabilité de sécurité pour les traitements irréguliers de ses employés effectués dans le cadre de leurs fonctions, même à des fins propres, ceci enlèverait une partie de son effet utile du RGPD et de la protection des données à caractère personnel.

65. La Chambre souligne néanmoins qu'indépendamment de la question de savoir qui est responsable de traitement pour les consultations abusives, c'est l'obligation de la défenderesse en sa qualité de responsable de traitement d'assurer la sécurité des données et des traitements qui constitue le cœur de cette décision. Dans le cas d'espèce, la défenderesse ne conteste pas son obligation d'assurer la sécurité des accès par ses employés au registre CCP et plus largement aux données de la BNB. Cet aspect sera développé ci-dessous.

II.2- Quant au principe de responsabilité et à l'obligation d'assurer la sécurité des données à caractère personnel

II.2.1- Principe de responsabilité

66. L'article 24.1 RGPD stipule que « compte tenu de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés de personnes physiques, le responsable du traitement met en œuvre les mesures techniques et organisationnelles appropriées pour s'assurer et être en mesure de démontrer que le traitement est effectué conformément au présent règlement. Ces mesures sont réexaminées et actualisées si nécessaire. ». Cet article traduit le principe de responsabilité, ou d' « accountability » énoncé à l'article 5.2. RGPD, selon lequel « Le responsable du traitement est responsable du respect du paragraphe 1 et est en mesure de démontrer que celui-ci est respecté (responsabilité). »

67. L'article 24.2. du RGPD précise que lorsque cela est proportionné au regard des activités de traitement, les mesures évoquées à l'article 24.1. du RGPD ci-dessus comprennent la mise en œuvre de politiques appropriées en matière de protection des données par le responsable de traitement.

68. Le considérant 74 du RGPD ajoute qu' « Il y a lieu d'instaurer la responsabilité du responsable du traitement pour tout traitement de données à caractère personnel qu'il effectue lui-même ou qui est réalisé pour son compte. Il importe, en particulier, que le responsable du traitement soit tenu de mettre en œuvre des mesures appropriées et effectives et soit à même de démontrer la conformité des activités de traitement avec le présent règlement, y compris l'efficacité des mesures. Ces mesures devraient tenir compte de la nature, de la portée, du contexte et des

finalités du traitement ainsi que du risque que celui-ci présente pour les droits et libertés des personnes physiques ».

69. Il lui incombe également, en application de l'article 25 du RGPD (protection des données dès la conception et par défaut), d'intégrer le nécessaire respect des règles du RGPD en amont de ses actes et procédures (par exemple s'assurer de l'existence et l'effectivité de procédures de contrôle pour les collaborateurs mais aussi les cadres dans leur accès aux données de la CCP).

70. Par ailleurs, le responsable de traitement est tenu, sur base de l'article 32 RGPD, d'assurer la sécurité des traitements, « compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques ». Or, la Chambre Contentieuse constate un manque de respect de l'obligation d'assurer le sécurité de traitement dans le chef de la défenderesse, qui fait partie du principe de responsabilité. Ce manquement est développé infra.

71. Ce manquement à l'obligation d'assurer la sécurité des traitements constitue le point d'ancrage de la présente décision et des sanctions qu'elle impose. L'absence des mesures techniques et organisationnelles permettant de limiter l'accès non justifié et insuffisamment sécurisé par un employé à la base de données CCP de la BNB, et a fortiori l'absence d'un système de contrôle ex post sur les accès ayant eu lieu, est considéré comme une infraction sérieuse. Le poste de cadre occupé par cet employé ne peut justifier cette absence de mesures de sécurité.

II.2.2-L'obligation de sécurité des données à caractère personnel et la journalisation des logs IT

a- Les contours de l'obligation de sécurité

72. 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». 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[16], à fortiori au vu du rôle crucial joué par les technologies de l'information et de la communication dans notre société.

[16] Le rôle crucial joué par la sécurité des données pour l'exercice effectif de leurs droits par les personnes concernées a été consacrée notamment par la CEDH dans son arrêt du 17 juillet 2008, I. c. Finlande, req. n° 20511/03, dans lequel la Cour conclut à l'unanimité à une violation de l'article 8 par les autorités Finlandaises,

73. Comme indiqué supra, le manquement à l'obligation d'assurer la sécurité des traitements constitue le cœur de décision. L'impact en termes de respect du droit à la protection de la vie privée de la plaignante lié à l'absence des mesures techniques et organisationnelles permettant de limiter l'accès non justifié et insuffisamment sécurisé par un employé à la base de données CCP de la BNB se voit par ailleurs renforcé par l'absence de possibilité de traçabilité ex post des consultations opérées. La Chambre Contentieuse rappelle que la lecture combinée des articles 32 (obligation d'assurer la sécurité des traitements), ainsi que 5.2 et 24 RGPD (soumettant le responsable du traitement au principe de responsabilité) impose au responsable du traitement de démontrer son respect de l'article 32, en prenant des mesures techniques et organisationnelles appropriées, de façon transparente et traçable. La tenue d'un registre journal des logs IT, ou « journalisation » s'articule autour de ces obligations, plus particulièrement de la traçabilité des traitements, et contribue à la nécessaire « disponibilité »[17] des données traitées.

74. La Chambre Contentieuse rappelle par ailleurs, le prescrit de l'article 25 (protection des données dès la conception et par défaut), qui impose au responsable de traitement d'intégrer le nécessaire respect des règles du RGPD en amont de ses actes et procédures (par exemple s'assurer de l'existence et l'effectivité de procédures de contrôle pour les collaborateurs mais aussi les cadres dans leur accès aux données de la CCP).

75. Il convient de relever que le principe de sécurité avec ses différentes composantes d'intégrité, confidentialité[18] et disponibilité[19] est repris aux articles 5.1.f) et 32 du RGPD et est désormais érigé dans le RGPD au même rang que les principes fondamentaux de licéité, transparence et loyauté.

76. Les obligations des responsables de traitement quant à la sécurité des traitements reposent dans les articles 32 et suivants du RGPD.

77. Les composantes classiques des recommandations en termes de sécurité de l'information, telles que préconisées par la suite ISO27xxx[20] sont la confidentialité des données, leur intégrité et leur

sur base d'une protection insuffisante contre les accès non autorisés du dossier médical d'une infirmière séropositive.

[17] Article 32.1.a RGPD

[18] Selon le Groupe 29 l'intégrité des données correspond à « la qualité en vertu de laquelle les données sont authentiques et n'ont pas été modifiées par mégarde ou malveillance pendant le traitement, le stockage ou la transmission. La notion d'intégrité peut s'étendre aux systèmes informatiques et exige que le traitement des données à caractère personnel sur ces systèmes reste inaltéré » Groupe 29, WP 196, Opinion 05/2012 on Cloud Computing, p. 18.

[20] La suite de normes ISO27xxx constitue un des principaux standards internationaux de sécurité de l'information.

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) »[21] .

78. L'imputabilité s'exprime notamment de façon concrète par la tenue d'un registre des log files.

79. La journalisation consiste donc à l'enregistrement 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.

80. Bien que la journalisation ne soit pas expressément mentionnée dans le RGPD[22], 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 par la Chambre Contentieuse à tout responsable de traitement. Ces mesures doivent être adaptées aux risques.

81. L'institution prédécesseur de l'APD (la Commission de la Vie Privée ; ci-après CPVP) indiquait déjà dans ses Lignes directrices pour la sécurité de l'information de données à caractère personnel[23] ainsi que dans sa Recommandation[24] aux villes et communes[25] concernant les registres de logs

---

[21] Dumortier, F., « Chapitre 4 - Cybersécurité, vie privée, imputabilité, journalisation et log files » in Les obligations légales de cybersécurité et de notifications d'incidents, Bruxelles, Politeia, 2019, p. 187 et APD, « Note relative à la sécurité des données à caractère personnel », p2.

[22] A l'inverse, la Directive (UE) 2016/680 accorde une importance particulière à la consultation et la divulgation (traitement les plus courants). et impose l'identification de l'auteur du traitement ainsi que celle des destinataires en cas de divulgation, le moment exacte , ainsi que la justification du traitement (du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données).

[23] Disponibles sur le lien https://www.autoriteprotectiondonnees.be/publications/lignes-directrices-pour-la-securite-de-l-information.pdf.

[24] Recommandation aux villes et communes concernant l'enregistrement du motif de la consultation du Registre national par les membres de leur personnel (CO-AR-2017-013), 30 août 2017, p7

[25] Dans cette recommandation aux villes et communes concernant la journalisation, la CPVP souligne l'importance de la journalisation comme « élément incontournable de toute politique de sécurité de l'information » et indique :

« *21. L'élaboration d'une politique de sécurité de l'information adéquate est nécessaire afin de prendre des mesures qui excluent tout accès non autorisé, et ce d'une manière documentée permettant à la commune d'assumer sa responsabilité. Dans ses mesures de référence en matière de sécurité applicables à tout traitement de données à caractère personnel, la Commission a déjà souligné que la mise en place d'un mécanisme sélectif de recherche et de journalisation constitue un élément incontournable de toute politique de sécurité de l'information.(…) ces lignes directrices prescrivent que tout accès au système informatique doit être traçable afin de vérifier qui a eu accès, quand, à quoi et pour quel motif.*

(…)

IT que la journalisation constitue un élément incontournable de toute politique de sécurité de l'information, en ce qu'elle permet la traçabilité des accès aux systèmes informatiques[26].

b- Lien entre les obligations de sécurité des responsables de traitement et les principes de responsabilité et transparence

82. La Chambre Contentieuse rappelle que l'article 32 RGPD doit être lu en combinaison avec l'article 5.2 RGPD et l'article 24 RGPD précités, soumettant le responsable du traitement au principe de responsabilité. Il incombe au responsable du traitement de démontrer son respect des dispositions du RGPD, en prenant des mesures techniques et organisationnelles appropriées, de façon transparente et traçable, permettant en cas de contrôle d'apporter la preuve des garanties appliquées.

83. 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[27].

84. 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."

85. 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:

86. « 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

---

23. Enfin, la Commission elle-même a déjà indiqué à plusieurs reprises que l'enregistrement du motif de la consultation du Registre national revêt une importance cruciale. Dans ses recommandations relatives à la gestion des accès et des utilisateurs dans le secteur public et à la communication d'informations contenues dans les registres de la population, la Commission souligne l'importance d'un traçage complet (qui, quoi, quand, pourquoi) impliquant une journalisation de chaque consultation des registres de la population, de manière à ce que toute consultation des données pour une finalité non légitime ou à titre personnel puisse être détectée et sanctionnée. Par extension, cette obligation est aussi valable pour la consultation et la mise à jour du Registre national. » (p8) (la Chambre souligne)

[26] Bien que cette recommandation s'adresse aux communes et villes, le raisonnement s'applique aux autres types de traitements de données, à fortiori lorsqu'il s'agit de données sensibles.

[27] Voir le considérant 78 du RGPD.

(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). »[28] (p. 10) (nous soulignons)

87. **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.**

88. Comme indiqué supra, l'effectivité des droits fondamentaux à la vie privée et à la protection des données à caractère personnel dépend considérablement des mesures mises en place pour assurer la sécurité de celles-ci[29], la tenue d'un registre des logs, bien que non imposée telle quelle par le RGPD, est donc encouragée par la Chambre Contentieuse.

89. Ceci vaut à fortiori pour les organismes de crédit, dans la mesure où la loi leur impose une consultation de l'état de crédit des personnes concernées à la BNB avant l'octroi d'un crédit.

II.2.3- Application au cas d'espèce

90. A la lumière de ce qui précède, et particulièrement dans la mesure où la consultation des données personnelles relatives aux crédits des personnes concernées constitue un traitement invasif de données financières sensibles, la Chambre Contentieuse estime que les mesures mises en place doivent être d'autant plus adaptées que les risques pour les droits fondamentaux des personnes concernées sont élevés.

91. L'importance de ces risques comme facteur est soulignée dans plusieurs articles pertinents du RGPD, y compris les articles 24, 25 et 32.

92. Pourtant, en l'espèce, un employé de la défenderesse a pu procéder à 20 reprises à des consultations illicites de ces données financières sensibles, sur une période s'étalant d'avril 2016 à août 2018.

---

[28] Recommandation aux villes et communes concernant l'enregistrement du motif de la consultation du Registre national par les membres de leur personnel (CO-AR-2017-013), 30 août 2017, p10. Dans le même sens, voir décision du Comité Sectoriel du Registre national du 11/01/2012.

[29] Dumortier, F., « Chapitre 4 - Cybersécurité, vie privée, imputabilité, journalisation et log files » in Les obligations légales de cybersécurité et de notifications d'incidents, Bruxelles, Politeia, 2019, p 141

93. Ceci, combiné à l'absence de tenue d'un registre journal des accès ou d'un quelconque contrôle des accès par les cadres (dont faisait partie l'ex-mari) aux registres de la BNB par la défenderesse avant l'incident, démontre l'insuffisance des mesures dans le chef de la défenderesse.

94. Lors de l'audition, bien qu'elle ait souligné l'existence d'un registre journal des accès des collaborateurs non cadres ainsi que le règlement déontologique interdisant toute utilisation abusive des accès, la DPO de la défenderesse a confirmé l'absence d'un quelconque système de contrôle des accès des cadres.

95. Ceci constitue une violation flagrante de l'article 32 RGPD (sécurité du traitement), lu en combinaison avec l'article 5.2 RGPD et l'article 24 RGPD.

96. Cette absence de journalisation ou d'autres mesures de sécurité dans le chef de la défenderesse empêche aussi la plaignante de pouvoir exercer son droit d'accès concernant les traitements illicites effectués par son ex-mari, employé de la défenderesse, puisque la défenderesse n'en conserve aucune trace.

97. Le SPL de l'APD a en effet demandé à la défenderesse dans son courrier du 5 septembre 2019 de communiquer à la plaignante la liste des consultations et des données concernées, ainsi que l'identité de l'auteur de ces consultations.

98. Cet aspect d'exercice du droit d'accès est développé infra (voir point II.4).

99. La défenderesse avance par ailleurs que « de nombreuses mesures ont été mises en place (…) afin de diminuer autant que possible le risque de consultations illégitimes de la Centrale de Crédits aux Particuliers par les membres de son personnel ».[30]

100. Elle fait état de ces mesures, et avance qu'elles ont été renforcées suite à la consultation abusive par l'ex-mari de la plaignante.

101. Elle cite ainsi :

- sélection du personnel sur base d'honorabilité et formation du personnel relative à la sécurité (y compris un examen pour les collaborateurs ayant accès aux données de la CCP) ;
- limitations techniques pour l'accès aux données de la CCP :

[30] Conclusions additionnelles et de synthèse de la défenderesse, p12.

- un dossier de crédit doit exister ;
- si accès via le système réservé aux collaborateurs non cadres, la consultation et l'identité du collaborateur est enregistrée ;
- si accès via le site de la CCP (réservé aux cadres), cet accès est uniquement possible via les ordinateurs des cadres, et un identifiant et mot de passe (unique pour tous les cadres de la SA) est nécessaire ;

- contrôles humains à plusieurs niveaux.

102. Il n'en demeure pas moins que la plaignante peut être suivie lorsqu'elle relève que la défenderesse admet dans ses conclusions que pour ses cadres, alors que ceux-ci disposent d'accès étendus aux données dans la CCP certes aux seules finalités suivantes : « corrections à réaliser dans les données encodées dans la CCP, la consultation des coordonnées du médiateur en cas de règlement collectif de dettes, et l'opération appelée « clean BNB », à savoir la comparaison des données reprises dans la CCP avec les fichiers de la défenderesse »[31].

103. Il n'y a aucun système de contrôle des consultations des données à la CCP.

104. La défenderesse spécifie elle-même à cet égard que pour les cadres, il est impossible d'identifier la personne précise qui a consulté les données.

105. La défenderesse le reconnaît d'ailleurs implicitement lorsqu'elle fait valoir que depuis les consultations illicites dénoncées par la plaignante, une série de mesures additionnelles ont été mises en place au sein de la société (dont une formation au RGPD des cadres, renforcement des contrôles de première ligne (c'est-à-dire des collaborateurs non cadres)).

106. Surtout vis-à-vis des cadres, la DPO de la défenderesse, interrogée lors de l'audition sur les mesures de sécurité prises concernant spécifiquement l'accès des cadres aux registres de la BNB depuis l'incident, explique que l'accès est dorénavant limité à deux superviseurs (au lieu de cinq comme auparavant), et que le mot de passe a été changé à deux reprises (une fois en 2019 et une fois en 2020).

107. Elle ajoute que la défenderesse a demandé en fin d'année 2020 (donc récemment), à la BNB de lui communiquer sa propre liste des accès afin de pouvoir comparer celle-ci avec la liste tenue par les deux cadres ayant accès aux registres de la BNB, afin d'identifier d'éventuelles différences dans un but de contrôle de l'activité des cadres

[31] Conclusions additionnelles et de synthèse p10.

108. La Chambre Contentieuse prend note des efforts fournis, qui par ailleurs restent à ses yeux insuffisants en ce qui concerne les cadres ayant accès aux registres de la BNB, sans pour autant que cela n'influence le manquement à son obligation de sécurité – conformément au principe de responsabilité - dans le chef de la défenderesse.

109. Elle constate aussi qu'aucune preuve de ces mesures additionnelles ne lui a été communiquée.

110. La défenderesse relève de plus qu'elle effectue chaque année des dizaines de milliers de consultations CCP en toute licéité, et que le nombre de consultations illicites est limité à 20, étalées entre avril 2016 et août 2018.

111. La Chambre Contentieuse en prend acte, mais rappelle que ceci n'enlève pas aux consultations leur caractère illicite ni répété, à des données personnelles financières sensibles.

112. La Chambre Contentieuse constate que la défenderesse était et demeure en défaut de mettre en œuvre les mesures techniques et organisationnelles adéquates requises par l'article 24.1 et 2 du RGPD pour garantir non seulement la sécurité des données en évitant des consultations illicites, mais aussi un exercice effectif des droits des personnes concernées telles la plaignante en l'absence de journalisation.

113. La défenderesse souligne par ailleurs que la plaignante a pour la première fois fait référence à une « intrusion » auprès d'elle 7 mois après la dernière consultation illicite, bien qu'elle en était déjà informée depuis 4 mois. Ceci n'est pas pertinent, dans la mesure où la plaignante est libre d'exercer ses droits à tout moment.

114. La défenderesse a donc violé l'article 32, lu en combinaison avec les articles 5.2 et 24 du RGPD.

II.3- Quant au respect des principes de finalité, transparence, et information

II.3.1- Sur les principes de loyauté, transparence, et information

115. En application de l'article 5.1, a), les données à caractère personnel doivent être « traitées de manière licite, loyale et transparente au regard de la personne concernée (licéité, loyauté, transparence) ».

116. Par ailleurs, en application des articles 13 et 14 du RGPD, toute personne dont des données à caractère personnel sont traitées doit, selon que les données sont collectées directement auprès

d'elle ou auprès de tiers, être informée des éléments listés à ces articles (§§ 1 et 2)[32]. En cas de collecte directe de données auprès de la personne concernée, celle-ci sera informée tant des éléments listés à l'article 13.1 et 2 du RGPD soit :

- de l'identité et des coordonnées du responsable de traitement ainsi que des coordonnées du délégué à la protection des données éventuel
- des finalités du traitement ainsi que de la base juridique de celui-ci (lorsque le traitement se fonde sur l'intérêt légitime du responsable de traitement, cet intérêt devra être précisé)
- des destinataires ou catégories de destinataires du traitement
- de l'intention du responsable de traitement de transférer les données hors de l'Espace Economique Européen
- de la durée de conservation des données,
- des droits que lui confère le RGPD en ce compris le droit de retirer son consentement à tout moment et celui de déposer une plainte auprès de l'autorité de contrôle de protection des données (en l'espèce l'APD
- des informations sur la question de savoir si l'exigence de fourniture de données à caractère personnel a un caractère réglementaire ou contractuel et les conséquences de leur non-fourniture ainsi que de l'existence d'une prise de décision automatisée y compris un profilage, visé à l'article 22 du RGPD.

117. La Chambre Contentieuse rappelle par ailleurs qu'en cas de collecte directe (article 13 du RGPD), aucune exception n'est prévue.

118. L'article 14.1 et 2 liste des éléments qui sont similaires tenant compte toutefois que l'hypothèse visée à l'article 14 du RGPD est celle où des données ne sont pas collectées directement auprès de la personne concernée mais bien auprès de tiers.

119. Ces informations sont, que ce soit sur la base de l'article 13 ou de l'article 14 du RGPD à fournir à la personne concernée dans le respect des modalités fixées à l'article 12 du RGPD.

II.3.2- La position de la plaignante quant à l'application des principes de loyauté, transparence et information

[32] Dans les lignes directrices qu'il a consacrées au principe de transparence (point 13), le Groupe 29 énonce ainsi : « (…) la position du G29 est qu'il n'y a pas de différence entre le statut des informations à fournir au titre du paragraphe 1 et du paragraphe 2 des articles 13 et 14, respectivement. Toutes les informations contenues dans ces paragraphes sont d'égale importance et doivent être fournies à la personne concernée ». La Chambre Contentieuse a fait sienne cette position notamment dans sa décision 41/2020 (p19).

120. La plaignante souligne que la défenderesse, lorsqu'elle a pris connaissance via ses échanges avec la plaignante des consultations illicites effectuées par son employé, par ailleurs reconnues par celui-ci, s'est abstenue de lui fournir la grande majorité des informations au titre de l'article 14 RGPD. Elle lui a ainsi indiqué la finalité du traitement (consultation des données à la CCP en vertu de son obligation légale et dans le cadre de la gestion des contrats de crédits), mais ne lui a pas fait parvenir sa Charte de la vie privée. Elle n'a ainsi, à titre d'exemple, pas informé la plaignante de la durée de conservation des données.

121. La circonstance que la plaignante était déjà en possession de la liste des consultations (obtenus via la BNB), ne change rien au constat que la défenderesse ne lui a pas fourni les autres informations requises au titre de l'article 14, qu'elle était en mesure de lui fournir.

122. II.3.3- La position de la défenderesse quant à l'application des principes de loyauté, transparence et information

123. La défenderesse avance en premier lieu que la plaignante aurait demandé les informations au titre de l'article 14 dans ses conclusions pour la première fois, et n'aurait jamais exprimé cette demande dans les échanges entre parties auparavant. La Chambre Contentieuse est d'avis que ceci relève de la mauvaise foi, dans la mesure où le SPL de l'APD a formellement demandé à la défenderesse[33] de transmettre ces informations à la plaignante, demande restée sans suite.

124. Par ailleurs, l'article 14.3 du RGPD indique :

« Le responsable du traitement fournit les informations visées aux paragraphes 1 et 2:

a)dans un délai raisonnable après avoir obtenu les données à caractère personnel, mais ne dépassant pas un mois, eu égard aux circonstances particulières dans lesquelles les données à caractère personnel sont traitées;

b)si les données à caractère personnel doivent être utilisées aux fins de la communication avec la personne concernée, au plus tard au moment de la première communication à ladite personne; ou

c) s'il est envisagé de communiquer les informations à un autre destinataire, au plus tard lorsque les données à caractère personnel sont communiquées pour la première fois ». (nous soulignons)

[33] Courrier du 21 octobre 2019 du SPL.

125. Le responsable du traitement se doit donc de transmettre les informations requises de sa propre initiative, au lieu d'attendre que la demande soit formulée par la personne concernée. En l'espèce, dans la mesure où les données à caractère personnel devaient être utilisées aux fins de la communication avec la plaignante, ces informations auraient dû lui être transmises au plus tard au moment de la première communication entre les parties.

126. La défenderesse tente ensuite de se déresponsabiliser, en répétant son argument selon lequel elle n'est pas responsable du traitement pour les consultations illicites des données de la plaignante, et que l'obligation de fournir les informations au titre de l'article 14 RGPD reviendrait à l'ex-mari de celle-ci.

127. Comme indiqué supra, ce raisonnement ne peut être suivi.

128. La défenderesse est bien sous l'obligation du principe de transparence et d'informations (article 14 RGPD en l'espèce), article fondamental posant des obligations claires et essentielles à l'égard des responsables du traitement pour permettre aux personnes concernées d'exercer leurs droits.

129. En outre, la défenderesse explique qu'aucune trace n'est conservée dans le cadre du système de consultation des données à la CCP réservé aux cadres superviseurs, tel que l'ex-mari de la plaignante, et qu'elle est donc dans l'impossibilité matérielle de fournir des informations quant aux données consultées.

130. La Chambre Contentieuse est d'avis que ceci constitue un aveu, comme indiqué supra, des manquements de la défenderesse aux principes de responsabilité et de sécurité (articles 5.2 , 24 et 32 du RGPD).

131. Les arguments avancés par la défenderesse pour se défaire de son obligation de respect des principes de loyauté, transparence et information ne peuvent être retenus.

132. Partant, et dès lors que la défenderesse ne démontre pas que les informations que la défenderesse était bien en mesure de fournir (malgré l'impossibilité technique avancée de fournir la liste des données consultées par exemple) au titre de l'article 14 auraient été transmises à la plaignante, la Chambre Contentieuse en conclut que la défenderesse a manqué à son obligation d'information à l'égard de celle-ci.

133. La Chambre Contentieuse rappelle qu'un aspect primordial du principe de transparence mis en lumière aux articles 12, 13 et 14 du RGPD est que la personne concernée devrait être en mesure de déterminer à l'avance ce que la portée et les conséquences du traitement englobent

afin de ne pas être pris au dépourvu à un stade ultérieur quant à la façon dont ses données à caractère personnel ont été utilisées.

134. Les informations devraient être concrètes et fiables, elles ne devraient pas être formulées dans des termes abstraits ou ambigus ni laisser de place à différentes interprétations. Plus particulièrement, les finalités et fondements juridiques du traitement des données à caractère personnel devraient être clairs.

II.4- Quant à la facilitation des droits de la plaignante et son droit d'accès

135. L'article 12 du RGPD indique :

« 1. Le responsable du traitement prend des mesures appropriées pour fournir toute information visée aux articles 13 et 14 ainsi que pour procéder à toute communication au titre des articles 15 à 22 et de l'article 34 en ce qui concerne le traitement à la personne concernée d'une façon concise, transparente, compréhensible et aisément accessible, en des termes clairs et simples, en particulier pour toute information destinée spécifiquement à un enfant. Les informations sont fournies par écrit ou par d'autres moyens y compris, lorsque c'est approprié, par voie électronique. Lorsque la personne concernée en fait la demande, les informations peuvent être fournies oralement, à condition que l'identité de la personne concernée soit démontrée par d'autres moyens.

2. Le responsable du traitement facilite l'exercice des droits conférés à la personne concernée au titre des articles 15 à 22. Dans les cas visés à l'article 11, paragraphe 2, le responsable du traitement ne refuse pas de donner suite à la demande de la personne concernée d'exercer les droits que lui confèrent les articles 15 à 22, à moins que le responsable du traitement ne démontre qu'il n'est pas en mesure d'identifier la personne concernée. » (nous soulignons)

136. L'article 15 RGPD stipule quant à lui :

« 1. La personne concernée a le droit d'obtenir du responsable du traitement la confirmation que des données à caractère personnel la concernant sont ou ne sont pas traitées et, lorsqu'elles le sont, l'accès auxdites données à caractère personnel ainsi que les informations suivantes:

a)les finalités du traitement;

b)les catégories de données à caractère personnel concernées;

c)les destinataires ou catégories de destinataires auxquels les données à caractère personnel ont été ou seront communiquées, en particulier les destinataires qui sont établis dans des pays tiers ou les organisations internationales;

d)lorsque cela est possible, la durée de conservation des données à caractère personnel envisagée ou, lorsque ce n'est pas possible, les critères utilisés pour déterminer cette durée;

e)l'existence du droit de demander au responsable du traitement la rectification ou l'effacement de données à caractère personnel, ou une limitation du traitement des données à caractère personnel relatives à la personne concernée, ou du droit de s'opposer à ce traitement;

f)le droit d'introduire une réclamation auprès d'une autorité de contrôle;

g)lorsque les données à caractère personnel ne sont pas collectées auprès de la personne concernée, toute information disponible quant à leur source;

h)l'existence d'une prise de décision automatisée, y compris un profilage, visée à l'article 22, paragraphes 1 et 4, et, au moins en pareils cas, des informations utiles concernant la logique sous-jacente, ainsi que l'importance et les conséquences prévues de ce traitement pour la personne concernée.

2. Lorsque les données à caractère personnel sont transférées vers un pays tiers ou à une organisation internationale, la personne concernée a le droit d'être informée des garanties appropriées, en vertu de l'article 46, en ce qui concerne ce transfert.

3. Le responsable du traitement fournit une copie des données à caractère personnel faisant l'objet d'un traitement. Le responsable du traitement peut exiger le paiement de frais raisonnables basés sur les coûts administratifs pour toute copie supplémentaire demandée par la personne concernée. Lorsque la personne concernée présente sa demande par voie électronique, les informations sont fournies sous une forme électronique d'usage courant, à moins que la personne concernée ne demande qu'il en soit autrement.

4. Le droit d'obtenir une copie visé au paragraphe 3 ne porte pas atteinte aux droits et libertés d'autrui. »

137. La plaignante avance que la défenderesse n'aurait pas facilité l'exercice de ses droits, et quelle s'est montré réticente face à ses demandes d'explications (par exemple en ne transmettant pas les informations requises au titre de l'article 14) . La défenderesse répond que la plaignante n'a

pas demandé que ces informations lui soient transmises. Cette question ayant été discutée plus haut et l'argument de la défenderesse ayant été écarté, la Chambre Contentieuse renvoie au point II.3.

138. La plaignante affirme aussi qu'« Estimer que (la plaignante) n'a pas exercé son droit d'accès alors qu'elle a explicitement demandé des justifications sur les consultations relève d'une certaine mauvaise foi » (conclusions de la plaignante p.18).

139. Selon la position constante de la Chambre Contentieuse[34], la formulation d'une demande d'accès ou de l'exercice de tout autre droit – eût-elle été incomplète ou fondée sur une disposition erronée ou à l'appui d'une mauvaise compréhension ou interprétation du droit invoqué – ne peut servir de prétexte au responsable de traitement pour ne pas y donner une suite utile. Ceci doit être examiné au cas par cas.

140. Dans le cas d'espèce, à la lecture des emails échangés entre les parties, la Chambre Contentieuse est d'avis qu'il ne ressort pas suffisamment que la plaignante a demandé l'exercice de son droit d'accès. Dans ses emails, la plaignante demande en effet principalement des explications sur les procédures d'accès aux données de la CCP, et sur les sanctions contre un employé abusant de son accès au fichier, dont son ex-mari[35].

141. Néanmoins, bien qu'il convient de distinguer des emails demandant des explications quant aux procédures d'accès aux données de la CCP ainsi que sur les sanctions contre un employé abusant de son accès au fichier d'une demande d'accès à ses données personnelles, la Chambre Contentieuse rappelle que le SPL a formellement demandé à la défenderesse (pour le compte de la plaignante), dans son courrier du 21 octobre (pièce 4 de la plaignante), de faire parvenir à la plaignante les informations au titre de l'article 14 et de faire suite à son droit d'accès aux données détenues par la défenderesse. La défenderesse n'a pas fait suite à ce courrier.

---

[34] Voir notamment la décision de la Chambre Contentieuse 41/2020 du 29 juillet 2020

[35] On peut ainsi lire dans les emails de la plaignante à la DPO de la défenderesse, à titre d'exemple :

-« (…) Merci d'avoir pris considération de la gravité des faits. Cependant, je ne désire pas le renvoi pur et simple de mon ex-mari, j'aimerais juste que la sanction prise à son encontre lui fasse prendre conscience que par son comportement il m' apporté un préjudice financier… » (email du 08 avril 2019)

-« J'aimerais toutefois savoir qu'encourt un employé qui déroge au respect de la protection des données » (email du 13 mars 2019)

-« Quoiqu'il en soit avant d rendre ma plainte effective, je voudrais savoir ce qu'encourt mon ex-mari pour avoir commis cette intrusion dans ma vie privée. Puis je citerai son nom, ce qui vous permettra seulement de le sanctionner » (email du 5 avril 2019)

142. La défenderesse a donc violé l'article 15 RGPD en ne faisant pas suite à la demande d'accès de la plaignante.

II.5- Quant à l'indépendance de la Délégué à la Protection des Données

143. La plaignante avance que la Délégué à la Protection des Données (DPO) de la défenderesse ne remplit pas la condition d'indépendance ressortant de l'article 38.3 RGPD, en raison de son parcours professionnel antérieur, du cumul de ses fonctions de DPO avec celles de CISO (Chief Information Security Officer), et en raison du fait qu'elle aurait « représenté les intérêts » de la défenderesse lors de ses interactions avec la plaignante. Ces arguments sont examinés successivement ci-dessous.

II.5.1-Le parcours professionnel de la DPO n'entraine pas de conflit d'intérêt

144. La plaignante soutient que la DPO aurait été antérieurement la directrice du service juridique de la défenderesse. Or, la défenderesse explique que la DPO a bien occupé cette fonction, mais au sein de la compagnie « W », n'ayant aucun lien avec elle. Cet argument est donc rejeté.

II.5.2-Le cumul de fonctions de DPO et CISO n'entraine pas de conflit d'intérêt

145. L'article 38.6 RGPD stipule que « Le délégué à la protection des données peut exécuter d'autres missions et tâches. Le responsable du traitement ou le sous-traitant veillent à ce que ces missions et tâches n'entraînent pas de conflit d'intérêts ».

146. Les lignes directrices de l'EDPB enseignent que le DPO « 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. »[36]

147. Il s'agit donc d'un conflit d'intérêts substantiel, pouvant surgir notamment lorsque la même personne est susceptible d'agir à la fois en position de contrôleur et de contrôlé (par exemple un responsable de projet ou département impliquant un traitement de données, qui exercerait à la fois la fonction de DPO alors qu'il serait amené en cette qualité à contrôler la conformité du traitement dans le cadre de son projet).

[36] EDPB, Lignes directrices concernant les délégués à la protection des données (DPD), 5 avril 2017, p19

148. Il s'agit notamment de prendre en compte le pouvoir décisionnel ou non qu'a le délégué à la protection des données dans l'exercice de son autre fonction[37].

149. La plaignante soulève un conflit d'intérêt dans le cumul des fonctions de DPO et CISO par une même personne au sein de la défenderesse car celle-ci exercerait un pouvoir de décision quant aux mesures techniques et organisationnelles mises en place au sein de la SA, mesures que la plaignante estime insuffisante et contraires à l'article 32 RGPD.

150. La défenderesse explique dans ses conclusions ainsi que lors de l'audition que les fonctions de DPO et de CISO ne sont pas des fonctions exécutives, mais des fonctions de conseil, d'identification de risques. Lors de l'audition, la DPO de la défenderesse a explicité qu'elle présente, au management de l'entreprise, les risques et leur importance et qu'il revient à ce management de décider si les mesures mises en place sont suffisantes pour remédier aux risques. Elle a par ailleurs précisé qu'en cas de désaccord entre elle et le management concernant les mesures prises et nonobstant les remarques adressées à ce dernier, la décision n'est pas de son ressort. Elle précise en outre que les mesures de sécurité relèvent de la direction informatique, et non pas de celle du CISO.

151. Elle indique aussi que dans l'organigramme de la SA défenderesse, les fonctions de CISO et DPO ressortent de la « deuxième ligne de défense », la première étant constituée par les fonctions opérationnelles, à l'inverse de la seconde.

152. Dans la mesure où le CISO n'est pas, dans le cas d'espèce, responsable d'un département opérationnel[38], la plaignante ne peut être suivi lorsqu'elle avance que la personne étant à la fois DPO et CISO exerce un pouvoir de décision quant aux mesures techniques et organisationnelles mises en place au sein de la défenderesse.

II.5.3-La teneur des réponses de la DPO à la plaignante n'indique pas une violation de son rôle

153. L'article 38.4 RGPD indique que « Les personnes concernées peuvent prendre contact avec le délégué à la protection des données au sujet de toutes les questions relatives au traitement de leurs données à caractère personnel et à l'exercice des droits que leur confère le présent règlement ».

154. Le DPO agit donc, entre autres, comme point de contact pour les personnes qui souhaitent exercer leurs droits auprès du responsable de traitement.

---

[37] Rosier, K., « Délégué à la protection des données :une fonction multifacette» in *Le règlement général sur la protection des données (RGPD/GDPR)*, Bruxelles, Éditions Larcier, 2018, p.578

[38] A l'inverse, la Chambre Contentieuse a estimé qu'il y a conflit d'intérêt dans le cas où un DPO est à la fois responsable de plusieurs départements opérationnels (voir décision 18/2020 p15 s)

155. La plaignante avance que la DPO aurait pris fait et cause pour la défenderesse (son employeur), au lieu d'instruire la plainte formulée par la plaignante de façon indépendante. Ce faisant, la plaignante se base sur la teneur des réponses formulées par la DPO aux emails de la plaignante, dont il ressort qu'elle utilise les termes « nous » (« nous ne pouvons vous donner plus d'informations », « nous avons présenté nos excuses », « nous avons bien entendu pris les mesures coercitives » …).

156. Or, bien que la plaignante ait exprimé sa frustration quant à la qualité de l'accompagnement de la DPO pour la facilitation de ses droits, il ne ressort pas de l'analyse des échanges écrits entre la plaignante et la DPO que celle-ci ne se serait pas comporté en conformité avec son rôle. Comme la DPO l'a indiqué lors de l'audition, les demandes de la plaignante s'axaient principalement sur la sanction encourue par son ex-mari, ce qui ne relève pas des données personnelles de la plaignante. La Chambre Contentieuse rappelle par ailleurs que la DPO est tenue au devoir de confidentialité (article 38.5), et suit celle-ci lorsqu'elle explique à l'audition qu'elle ne pouvait pour cette raison pas répondre à la plaignante concernant les sanctions encourues par son ex-mari.

157. En conclusion, la plaignante ne peut être suivie lorsqu'elle avance que la DPO ne remplit pas la condition d'indépendance en raison de son parcours professionnel antérieur, du cumul de ses fonctions de DPO avec celles de CISO, et en raison du fait qu'elle aurait « représenté les intérêts » de la défenderesse lors de ses interactions avec la plaignante.

158. Il n'y a donc pas de violation de l'article 38 RGPD.

4. Quant aux mesures correctrices et aux sanctions

4.1- Les mesures correctrices et sanctions

Aux termes de l'article 100 LCA, la Chambre Contentieuse a le pouvoir de :

1° classer la plainte sans suite ;

2° ordonner le non-lieu ;

3° prononcer une suspension du prononcé ;

4° proposer une transaction ;

5° formuler des avertissements ou des réprimandes ;

6° ordonner de se conformer aux demandes de la personne concernée d'exercer ces droits;

7° ordonner que l'intéressé soit informé du problème de sécurité;

8° ordonner le gel, la limitation ou l'interdiction temporaire ou définitive du traitement;

9° ordonner une mise en conformité du traitement;

10° ordonner la rectification, la restriction ou l'effacement des données et la notification de celles-ci aux récipiendaires des données;

11° ordonner le retrait de l'agréation des organismes de certification;

12° donner des astreintes;

13° donner des amendes administratives;

14° ordonner la suspension des flux transfrontières de données vers un autre Etat 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.

159. L'article 100 précité spécifie la liste des sanctions de l'article 58.2 du RGPD.

Quant à l'amende administrative qui peut être imposée en exécution de l' articles 83 du RGPD et des articles 100, 13° et 101 LCA, l'article 83 du RGPD prévoit :

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

2. Selon les caractéristiques propres à chaque cas, les amendes administratives sont imposées en complément ou à la place des mesures visées à l'article 58, paragraphe 2, points a) à h), et j). Pour décider s'il y a lieu d'imposer une amende administrative et pour décider du montant de l'amende administrative, il est dûment tenu compte, dans chaque cas d'espèce, des éléments suivants :

a) la nature, la gravité et la durée de la violation, compte tenu de la nature, de la portée ou de la finalité du traitement concerné, ainsi que du nombre de personnes concernées affectées et le niveau de dommage qu'elles ont subi;

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

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

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

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

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

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

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

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

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

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

160. Il importe de contextualiser le manquement aux articles 32, combiné aux articles 5 et 24, et 15 RGPD en vue d'identifier les mesures correctrices les plus adaptées.

161. Dans ce cadre, la Chambre Contentieuse tiendra compte de l'ensemble des circonstances de l'espèce, en ce compris - dans les limites qu'elle précise ci-après - de la réaction communiquée par la défenderesse au montant d'amende envisagée qui lui a été communiqué (voir rétroactes de la procédure). A cet égard, la Chambre Contentieuse précise que ledit formulaire mentionne expressément qu'il n'implique pas de réouverture des débats. Il poursuit comme seul but de recueillir la réaction de la défenderesse sur le montant de l'amende envisagée.

162. La Chambre Contentieuse tient également à préciser qu'il lui appartient souverainement en qualité d'autorité administrative indépendante - dans le respect des articles pertinents du RGPD et de la LCA - de déterminer la/les mesure(s) correctrice(s) et sanction(s) appropriée(s).

163. Ainsi, il n'appartient pas à la plaignante de solliciter de la Chambre Contentieuse quelle ordonne telle ou telle mesure correctrice ou sanction. Si, nonobstant ce qui précède, le/la plaignant(e) devait néanmoins demander à la Chambre Contentieuse qu'elle prononce l'une ou l'autre mesure et/ou sanction, il n'incombe pas dès lors à cette dernière de motiver pourquoi elle ne retiendrait pas l'une ou l'autre demande formulée par le/la plaignant(e). Ces considérations laissent intacte

l'obligation pour la Chambre Contentieuse de motiver le choix des mesures et sanctions auxquelles elle juge, (parmi la liste des mesures et sanctions mises à sa disposition par les articles 58 du RGPD et 100 de la LCA) approprié de condamner la partie mise en cause.

164. En l'espèce, la Chambre Contentieuse relève que la plaignante sollicite notamment de la Chambre Contentieuse qu'elle ordonne une mise en conformité au RGPD (notamment à l'article 32, combiné aux articles 5 et 24) des consultations du CCP des cadres.

165. La plaignante sollicite aussi l'imposition d'une amende administrative. La Chambre Contentieuse souligne qu'il lui revient de veiller à une application efficace des règles du RGPD. D'autres mesures, telles l'ordre de mise en conformité ou l'interdiction de poursuivre certains traitements par exemple, permettent quant à elles de mettre fin à un manquement constaté. Comme cela ressort du considérant 148 du RGPD, les sanctions, y compris les amendes administratives, sont infligées en cas de violations sérieuses, en complément ou à la place des mesures appropriées qui s'imposent. Dès lors, l'amende administrative peut assurément venir sanctionner un manquement grave auquel il aurait été remédié en cours de procédure ou qui serait sur le point de l'être. Il n'en demeure pas moins que la Chambre Contentieuse tiendra compte des mesures prises suite à l'incident dans la fixation du montant de l'amende.

4.2- Quant aux manquements

166. La Chambre Contentieuse a constaté un manquement à l'article 32, combiné aux articles 5 et 24, ainsi qu'à l'article 15 RGPD.

167. La Chambre Contentieuse prend par ailleurs acte du fait que la défenderesse a dès ses conclusions et lors de l'audition, reconnu qu'un manquement à l'article 32 peut lui être reproché[39]. Elle a par ailleurs explicité une mesure organisationnelle nouvelle instaurée suite à l'incident (seuls deux cadres disposent à présent des accès au registre CCP de la BNB, et ils en tiennent dorénavant un registre qui sera comparé à celui tenu par la BNB par mesure de contrôle).

168. Bien qu'elle prend acte de ces efforts, la Chambre Contentieuse est d'avis qu'ils ne sont pas suffisants et que d'autres mesures doivent être apportées par la défenderesse pour se mettre en conformité avec ses obligations découlant du RGPD. Partant, la Chambre Contentieuse lui impose un ordre de mise en conformité du processus des accès par les cadres au CCP. Elle recommande par ailleurs fortement la tenue d'un registre journal des accès, à comparer avec celui tenu par la BNB, et en conformité avec toutes les indications mentionnées supra (voir supra II.2.2).

[39] Conclusions additionnelles et de synthèse de Y p.9

169. La Chambre Contentieuse estime par ailleurs que la nature sensible des données traitées à grande échelle par la défenderesse aurait dû la mener à un renforcement de sa conformité aux principes susmentionnés du GDPR (dont la sécurité des traitements) bien avant, notamment par anticipation des risques liés à de tels manquements.

170. Outre cet ordre de mise en conformité, la Chambre Contentieuse est d'avis qu'en complément, une amende administrative est en l'espèce justifiée pour les motifs ci-après, motifs analysés sur base de l'article 83.2 RGPD et conformément à l'enseignement récent de la Cour des Marchés.[40]

171. Les droits des personnes concernées, ainsi que le principe de sécurité, font partie de l'essence du RGPD et leur violation sont punies des amendes les plus élevées, conformément à l'article 83.5 RGPD. Dans cet esprit, ces manquements sérieux peuvent être sanctionnés d'amendes proportionnellement élevées, en fonction des circonstances du cas d'espèce. A cet égard, on peut citer les Lignes directrices du Groupe 29 sur l'application et la fixation des amendes administratives[41], selon lesquelles :

« Les amendes sont un instrument important que les autorités de contrôle devraient utiliser dans les circonstances appropriées. Les autorités de contrôle sont encouragées à adopter une approche mûrement réfléchie et équilibrée lorsqu'elles appliquent des mesures correctives afin de réagir à la violation d'une manière tant effective et dissuasive que proportionnée. *Il ne s'agit pas de considérer les amendes comme un recours ultime ni de craindre de les imposer, mais, en revanche, elles ne doivent pas non plus être utilisées de telle manière que leur efficacité s'en trouverait amoindrie*. »

172. Dans son alinéa a), l'article 83.2. concerne « la nature, la gravité et la durée de la violation, compte tenu de la nature, de la portée ou de la finalité du traitement concerné, ainsi que du nombre de personnes concernées affectées et le niveau de dommage qu'elles ont subi ».

173. Dans le cas d'espèce, la Chambre Contentieuse relève que tant le principe de sécurité (article 5.1, f) RGPD) (et les obligations qui en découlent – article 32 du RGPD) que le droit d'accès (article 15), sont des principes essentiels du régime de protection mis en place par le RGPD. Le principe de responsabilité énoncé à l'article 5.2. du RGPD et développé à l'article 24 est par ailleurs au cœur du RGPD et traduit le changement de paradigme amené par celui-ci, soit un basculement d'un régime qui s'appuyait sur des déclarations et autorisations préalables de l'autorité de contrôle vers une plus grande responsabilisation et responsabilité du responsable de traitement. Le respect

[40] Cour d'appel de Bruxelles, 19eme chambre, section Cour des marchés, arrêt du 27 janvier 2021, p21-24

[41] Groupe 29, Lignes directrices sur l'application et la fixation des amendes administratives aux fins du règlement (UE) 2016/679, WP 253, adoptées le 3 octobre 2017, p7

de ses obligations par ce dernier et sa capacité à le démontrer n'en sont dès lors que plus importants. Les manquements à ces principes sont constitutifs de manquements graves.

174. Concernant plus spécifiquement la nature des données consultées de façon abusive, la Chambre souligne que la défenderesse est active dans le secteur bancaire et traite des volumes importants de données financières sensibles (des données relatives aux crédits des personnes concernées). Les données relatives aux crédits de la plaignante ont en l'espèce été consultées abusivement sur une période s'étendant d'avril 2016 à août 2018, et ce à pas moins de 20 reprises. La Chambre en conclut que les consultations abusives en question, tant par leur nature, que leur gravité et leur durée sont constitutives d'infractions sérieuses.

175. Elle note aussi qu'en l'absence de plainte introduite par la plaignante, il n'est pas déraisonnable de penser que de telles consultations abusives auraient pu continuer et rester impunies, puisque c'est suite à la plainte que la défenderesse a pris des mesures additionnelles et sanctionné son employé fautif.

176. Par ailleurs, la Chambre Contentieuse relève que les données personnelles de près de 6 millions de personnes figurent dans le registre CCP de la BNB, et que les employés de la défenderesse, dont les cadres, les consultent de façon régulière.

177. Quant à la question de savoir si les manquements ont été commis délibérément ou non (par négligence) (art. 83.2.b) du RGPD), la Chambre Contentieuse rappelle que « non délibérément » signifie qu'il n'y a pas eu d'intention de commettre la violation, bien que le responsable du traitement n'ait pas respecté l'obligation de diligence qui lui incombe en vertu de la législation. En l'espèce, la Chambre Contentieuse est d'avis que les manquements constatés - fussent-ils graves - ne traduisent pas une intention délibérée de violer le RGPD dans le chef de la défenderesse. L'alinéa d) de l'article 83.2 RGPD revient ensuite sur le degré de responsabilité du responsable du traitement, compte tenu des mesures techniques et organisationnelles (article 32 RGPD). La Chambre renvoi ici aux développements supra, desquels il ressort que la défenderesse n'avait mis en place aucune mesure de sécurité concernant l'accès des cadres aux données du registre CCP avant les consultations abusives. Il ressort aussi des déclarations de la DPO de la défenderesse que suite à cet incident, l'unique nouvelle mesure mise en place à cet effet reste limitée (réduction du nombre de cadres ayant accès au registre CCP de cinq à deux et tenue par ces cadres d'un registre des accès).

178. Enfin, l'article 83.2.e) concerne « toute violation pertinente commise précédemment par le responsable du traitement ou le sous-traitant ». La Chambre Contentieuse note à cet égard que le groupe dont fait partie la défenderesse a été sanctionné par une autre autorité de contrôle.

179. La Chambre note les efforts de la défenderesse concernant ses employés collaborateurs (nouvelle formation au RGPD, sensibilisation du personnel…) mais relève, comme indiqué supra, que les mesures de sécurité additionnelles spécifiques aux accès des cadres demeurent faibles. La seule mesure nouvelle suite à l'incident consiste en effet en une réduction de 5 à 2 cadres pouvant accéder au CCP. La Chambre remarque aussi que la défenderesse s'est seulement rendue compte en décembre 2020 de la possibilité de comparer la liste d'accès des cadres qu'elle tient (dorénavant) avec celle tenue par la BNB, alors que la plaignante a notifié les consultations abusives et qu'elles ont été reconnues par leur auteur (l'ex-mari de la plaignante) dès 2019.

180. La Chambre Contentieuse constate que les autres critères de l'article 83.2. du RGPD ne sont ni pertinents ni susceptibles d'influer sur sa décision quant à l'imposition d'une amende administrative et son montant. Aux termes de l'article 83.5 a) RGPD, les violations de toutes ces dispositions peuvent s'élever jusqu'à 20.000.000 d'euros ou dans le cas d'une entreprise, jusqu'à 4% du chiffre d'affaire annuel mondial total de l'exercice précédent. Les montants maxima d'amende pouvant être appliqués en cas de violation de ces dispositions sont supérieurs à ceux prévus pour d'autres types de manquements listés à l'article 83.4. du RGPD. S'agissant de manquements à un droit fondamental, consacré à l'article 8 de la Charte des droits fondamentaux de l'Union européenne, l'appréciation de leur gravité se fera, comme la Chambre Contentieuse a déjà eu l'occasion de le souligner, à l'appui de l'article 83.2.a) du RGPD, de manière autonome[42].

181. La Chambre Contentieuse rappelle le prescrit de l'article 83.4 RGPD, qui énumère les manquements pour lesquels l'amende peut s'élever 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 des deux étant d'application. Les manquements aux articles 8, 11, 25 à 39, 42 et 43 sont retenus. De telles infractions couvrent donc, entre autres, un manquement à l'obligation d'instaurer des mesures techniques et organisationnelles appropriées pour assurer la conformité au GDPR, un manquement à l'obligation de sécurité des traitements, à l'obligation de protection des données dès la conception et protection des données par défaut, ou encore à l'obligation de garder des registres des traitements. En l'espèce, comme indiqué supra, la Chambre Contentieuse relève tant un manquement à l'obligation d'instaurer des mesures techniques et organisationnelles appropriées pour assurer la conformité au GDPR, qu'à l'obligation de sécurité des traitements, ainsi qu'à l'obligation de protection des données dès la conception et protection des données par défaut . Le montant maximum de l'amende dans le cas d'espèce, telle que prévu par l'article 83.5 est donc de 10.000.000 EUR.

---

[42] Voy. la décision 64/2020 de la Chambre Contentieuse (point 54), disponible sur https://www.autoriteprotectiondonnees.be/publications/decision-quant-au-fond-n-64-2020.pdf

182. La défenderesse fait par ailleurs partie d'une grande multinationale, ce qu'elle a confirmé lors de l'audition. Dans sa détermination du montant de l'amende, la Chambre contentieuse tient compte de la notion d'entreprise (article 83. 5 du RGPD). La Chambre Contentieuse tient également compte de l'opinion du Comité Européen de la Protection des données dont elle retient tout particulièrement ce qui suit:

« *Pour infliger des amendes effectives, proportionnées et dissuasives, les autorités de contrôle s'en remettront à la définition de la notion d'entreprise fournie par la CJUE aux fins de l'application des articles 101 et 102 du traité FUE, à savoir que la notion d'entreprise doit s'entendre comme une unité économique pouvant être formée par la société mère et toutes les filiales concernées. Conformément au droit et à la jurisprudence de l'Union, il y a lieu d'entendre par entreprise l'unité économique engagée dans des activités commerciales ou économiques, quelle que soit la personne morale impliquée (considérant 150).* »

183. En conclusion, au regard des éléments développés ci-dessus propres à cette affaire, la Chambre Contentieuse estime que les manquement susmentionnés justifient qu'au titre de sanction effective, proportionnée et dissuasive telle que prévue à l'article 83 du RGPD et compte tenu des facteurs d'appréciation listés à l'article 83.2 RGPD et de la réaction de la défenderesse au formulaire d'amende envisagée, un ordre de mise en conformité assorti d'une amende administrative d'un montant de 100.000 euros (article 100.1, 13° et 101 LCA) soient prononcés à l'encontre de la défenderesse.

184. Le montant de 100.000 euros demeure eu égard à ces éléments proportionné aux manquements dénoncés. Ce montant demeure en outre largement inférieur au montant maximum prévu par l'article 83.5 RGPD, de 10.000.000 euros (voir supra).

185. Ce montant se justifie pour les raisons énoncées supra, y compris la nature sensible des données faisant l'objet des traitements litigieux (données financières relatives au crédit de la plaignante), la période étendue durant lequel les traitements ont eu lieu, ou encore le nombre de reprises élevées auquel ces traitements ont eu lieu (20). D'autres considérations justifiant ce montant se fondent sur le fait que peu de mesures additionnelles ont été mises en place depuis l'incident par la défenderesse pour renforcer la sécurité de ses traitements, sur le fait que sans l'introduction de la plainte, il n'est pas déraisonnable de penser que les consultations abusives auraient pu continuer sans que l'attention de la défenderesse ne soit attirée sur les failles dans ses mesures de sécurité, qui par ailleurs traite un volume important de données financières sensibles (6 millions de consultations au registre CCP par an, selon ses déclarations). La Chambre Contentieuse est d'avis qu'un montant d'amende inférieur ne rencontrerait pas, en l'espèce, les critères requis par l'article 83.1. du RGPD selon lesquels l'amende administrative doit être non seulement proportionnée, mais également effective et dissuasive. Ce éléments constituent une spécification de l'obligation

générale des États membres sous le droit de l'Union Européenne, basé sur le principe de coopération loyale (article 4.3 du Traité sur l'Union européenne).

186. Vu l'importance de la transparence concernant le processus décisionnel de la Chambre Contentieuse et conformément à l'article 100.1er, 16° de la LCA, la présente décision est publiée sur le site Internet de l'Autorité de protection des données en supprimant les données d'identification des parties, vu que celles-ci ne sont ni nécessaires ni pertinentes dans le cadre de la publication de la présente décision.

POUR CES MOTIFS,

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

- d'ordonner à la défenderesse, conformément à l'article 100, § 1er, 9° de la LCA, de mettre l'accès au registre CCP de la BNB par les employés cadres en conformité avec les articles 5.1.f et 32 du RGPD. À cet effet, la Chambre Contentieuse accorde à la défenderesse un délai de trois mois et attend qu'elle lui fasse un rapport dans le même délai concernant la mise en conformité du traitement avec les dispositions susmentionnées.

- en vertu de l'article 83 du RGPD et des articles 100, 13° et 101 de la LCA, d'infliger au défendeur une amende administrative de 100.000 euros pour violation des articles susmentionnés

En vertu de l'article 108.1 LCA, cette décision peut faire l'objet d'un recours auprès de la Cour des marchés (Cour d'appel de Bruxelles) dans un délai de 30 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