Chambre Contentieuse

Décision quant au fond 22/2020 du 8 mai 2020

Numéro de dossier : DOS-2018-02716

Objet : Violation de données à caractère personnel et obligation de conclure (en temps utile) un contrat de sous-traitance

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

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

Vu la loi du 3 décembre 2017 *portant création de l'Autorité de protection des données*, ci-après la 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 :

Y, ci-après : "le défendeur".

1. Faits et procédure

Le 4 juin 2018, le délégué à la protection des données du défendeur notifie une fuite de données à l'Autorité de protection des données, en vertu de l'article 114/1 de la loi du 13 juin 2005 *relative aux communications électroniques* et conformément au Règlement 611/2013 de la Commission européenne[1].

2. Le 6 juin 2018, le défendeur introduit à ce sujet une notification complémentaire auprès de l'Autorité de protection des données.

3. Dans sa notification, le défendeur mentionne que le 28 mai 2018, il a été informé par téléphone de ladite fuite de données par la *Computer Emergency Response Team* fédérale (ci-après "CERT") et que cette notification de la CERT a été confirmée par écrit le 29 mai 2018.

La fuite de données a eu lieu dans le cadre du *Master IT Service Agreement* conclu le 17 juin 2014 entre le défendeur et la société de droit indien *Z* (ci-après "le sous-traitant").

Au moyen de ce contrat, le sous-traitant a notamment été désigné pour convertir le magasin en ligne existant du défendeur, fonctionnant sur la base du système de *content management* Drupal 6, en un nouveau magasin en ligne fonctionnant sur Magento. En outre, il a également été demandé au sous-traitant d'analyser et de résoudre des problèmes de production existants relatifs au site Internet.

Pour le test du nouveau magasin en ligne et la solution de ces problèmes, le sous-traitant a placé une copie de la banque de données de production avec l'historique des commandes sur un cloud *Amazon Web Server* (AWS). Le sous-traitant a activé un serveur web sur le port 80 (HTTP) sur cet AWS et y a permis un accès libre en appliquant de mauvais paramètres de sécurité. De plus, le sous-traitant a activé le service "*Directory Listing*" sur ce serveur, permettant ainsi de naviguer dans l'intégralité de la structure de répertoire sur le serveur web.

[1] Règlement (UE) n° 611/2013 de la Commission du 24 juin 2013 *concernant les mesures relatives à la notification des violations de données à caractère personnel en vertu de la directive 2002/58/CE du Parlement européen et du Conseil sur la vie privée et les communications électroniques*, JO L 173/2.

Les données à caractère personnel de clients du défendeur ont ainsi été disponibles sur Internet entre le 22 mars 2018 et le 28 mai 2018. Une analyse forensique des fichiers de journalisation a révélé que les données ont été consultées et/ou téléchargées par des tiers.

D'après les informations reprises dans le formulaire de notification introduit par le défendeur auprès de l'Autorité de protection des données, il s'agissait plus particulièrement de données d'identification (nom, adresse, numéro de téléphone), de données d'identification électroniques (adresses IP), de numéros de Registre national et de numéros IBAN des personnes concernées. Le défendeur indique également dans ce formulaire de notification que la fuite de données concerne les données à caractère personnel de 32.153 personnes.

4. Par e-mail du 6 juin 2018, l'Autorité de protection des données, après concertation avec l'Institut belge des services postaux et des télécommunications (ci-après "IBPT"), pose plusieurs questions au défendeur concernant la fuite de données et plus particulièrement concernant la nature de cette fuite de données, la méthode d'évaluation des risques employée par le défendeur, le fondement juridique du traitement, l'information des personnes concernées et l'éventuelle implication d'autres États membres européens et autorités de contrôle européennes.

5. Par e-mail du 11 juin 2018, le délégué à la protection des données du défendeur répond à plusieurs des questions précitées.

Le défendeur transmet un projet de notification à adresser aux personnes concernées ainsi qu'un projet de communiqué de presse. Par ailleurs, le défendeur précise que le sous-traitant n'avait pas l'autorisation de copier les données vers un environnement qui n'est pas un environnement de production. Le défendeur communique également qu'aucune autre autorité de protection des données européenne n'a été informée.

6. Par e-mail du 12 juin 2018, l'Autorité de protection des données pose quelques questions complémentaires au défendeur.

Elle prie plus particulièrement le défendeur de transmettre une copie du contrat de sous-traitance ainsi que les résultats de l'audit de sécurité réalisé à l'égard du sous-traitant. L'Autorité de protection des données demande aussi si une analyse d'impact relative à la protection des données sera réalisée concernant les risques liés à la gestion des magasins en ligne du défendeur et si de nouveaux accords concrets ont été conclus avec le sous-traitant.

7. Le délégué à la protection des données du défendeur répond à ces questions par e-mail du 14 juin 2018.

8. Le 11 juillet 2018 , le Comité de direction de l'Autorité de protection des données décide, en vertu de l'article 63, 1° de la LCA, de saisir le Service d'Inspection du dossier étant donné qu'il constate des indices sérieux quant à l'existence d'une violation, d'une part de la responsabilité quant à l'évaluation du risque lors de la notification de la violation de données à caractère personnel, et d'autre part de l'obligation de conclure (en temps utile) un contrat de sous-traitance.

9. Par e-mail du 10 août 2018, le délégué à la protection des données du défendeur transmet les réponses de ce dernier aux questions posées par l'Autorité de protection des données le 10 juillet 2018.

10. Par courrier du 5 février 2019, l'Autorité de protection des données pose plusieurs questions supplémentaires au défendeur.

11. Le 22 février 2019, le délégué à la protection des données du défendeur transmet les réponses de ce dernier aux questions posées par l'Autorité de protection des données le 5 février 2019.

12. Le 12 août 2019, le Service d'Inspection transmet son rapport d'inspection au président de la Chambre Contentieuse, conformément à l'article 91, § 2 de la LCA.

13. Le 12 septembre 2019, la Chambre Contentieuse décide, en vertu de l'article 95, § 1er, 1° et de l'article 98 de la LCA, que le dossier peut être traité sur le fond.

14. Par courrier recommandé du 12 septembre 2019, le défendeur est informé du fait que la plainte peut être traitée sur le fond et, en vertu de l'article 99 de la LCA, il est également informé du délai pour introduire ses conclusions.

15. Le 14 octobre 2019, le défendeur dépose ses conclusions et demande à être entendu, conformément à l'article 98, 2° de la LCA.

16. Le 8 avril 2020, le défendeur est entendu par la Chambre Contentieuse, conformément à l'article 53 du règlement d'ordre intérieur.

17. Le 23 avril 2020, le procès-verbal d'audition est transmis au défendeur, conformément à l'article 54 du règlement d'ordre intérieur.

18. Le 28 avril 2020, le défendeur transmet ses remarques, qui sont annexées au procès-verbal d'audition, conformément à l'article 54, deuxième alinéa du règlement d'ordre intérieur.

2. Base juridique

Article 5.1.f) du RGPD

1. Les données à caractère personnel sont : (...)
f) traitées de façon à garantir une sécurité appropriée des données à caractère personnel, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées (intégrité et confidentialité) ;

Article 5.2 du RGPD

"2. Le responsable du traitement est responsable du respect du paragraphe 1 et est en mesure de démontrer que celui-ci est respecté (responsabilité)."

Article 24.1 du RGPD

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

Article 28.3 du RGPD

"3. Le traitement par un sous-traitant est régi par un contrat ou un autre acte juridique au titre du droit de l'Union ou du droit d'un État membre, qui lie le sous-traitant à l'égard du responsable du traitement, définit l'objet et la durée du traitement, la nature et la finalité du traitement, le type de

données à caractère personnel et les catégories de personnes concernées, et les obligations et les droits du responsable du traitement. Ce contrat ou cet autre acte juridique prévoit, notamment, que le sous-traitant :

a) ne traite les données à caractère personnel que sur instruction documentée du responsable du traitement, y compris en ce qui concerne les transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale, à moins qu'il ne soit tenu d'y procéder en vertu du droit de l'Union ou du droit de l'État membre auquel le sous-traitant est soumis; dans ce cas, le sous-traitant informe le responsable du traitement de cette obligation juridique avant le traitement, sauf si le droit concerné interdit une telle information pour des motifs importants d'intérêt public ;
b) veille à ce que les personnes autorisées à traiter les données à caractère personnel s'engagent à respecter la confidentialité ou soient soumises à une obligation légale appropriée de confidentialité ;
c) prend toutes les mesures requises en vertu de l'article 32 ;
d) respecte les conditions visées aux paragraphes 2 et 4 pour recruter un autre sous-traitant ;
e) tient compte de la nature du traitement, aide le responsable du traitement, par des mesures techniques et organisationnelles appropriées, dans toute la mesure du possible, à s'acquitter de son obligation de donner suite aux demandes dont les personnes concernées le saisissent en vue d'exercer leurs droits prévus au chapitre III ;
f) aide le responsable du traitement à garantir le respect des obligations prévues aux articles 32 à 36, compte tenu de la nature du traitement et des informations à la disposition du sous-traitant ;
g) selon le choix du responsable du traitement, supprime toutes les données à caractère personnel ou les renvoie au responsable du traitement au terme de la prestation de services relatifs au traitement, et détruit les copies existantes, à moins que le droit de l'Union ou le droit de l'État membre n'exige la conservation des données à caractère personnel ; et
h) met à la disposition du responsable du traitement toutes les informations nécessaires pour démontrer le respect des obligations prévues au présent article et pour permettre la réalisation d'audits, y compris des inspections, par le responsable du traitement ou un autre auditeur qu'il a mandaté, et contribuer à ces audits. 4.5.2016 L 119/49 Journal officiel de l'Union européenne
En ce qui concerne le point h) du premier alinéa, le sous-traitant informe immédiatement le responsable du traitement si, selon lui, une instruction constitue une violation du présent règlement ou d'autres dispositions du droit de l'Union ou du droit des États membres relatives à la protection des données."

Article 32 du RGPD

"1. 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, le responsable du traitement et le

sous-traitant mettent en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque, y compris entre autres, selon les besoins :
a) la pseudonymisation et le chiffrement des données à caractère personnel ;
b) des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement ;
c) des moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique ;
d) une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement. 2. Lors de l'évaluation du niveau de sécurité approprié, il doit être tenu compte en particulier des risques que présente le traitement, résultant notamment de la destruction, de la perte, de l'altération, de la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou de l'accès non autorisé à de telles données, de manière accidentelle ou illicite.
3. L'application d'un code de conduite approuvé comme le prévoit l'article 40 ou d'un mécanisme de certification approuvé comme le prévoit l'article 42 peut servir d'élément attestant du respect des exigences prévues au paragraphe 1 du présent article.
4. Enfin, Le responsable du traitement et le sous-traitant doivent prendre des mesures pour 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."

Article 33 du RGPD

"1. En cas de violation de données à caractère personnel, le responsable du traitement en notifie la violation en question à l'autorité de contrôle compétente conformément à l'article 55, dans les meilleurs délais et, si possible, 72 heures au plus tard après en avoir pris connaissance, à moins que la violation en question ne soit pas susceptible d'engendrer un risque pour les droits et libertés des personnes physiques. Lorsque la notification à l'autorité de contrôle n'a pas lieu dans les 72 heures, elle est accompagnée des motifs du retard.
2. Le sous-traitant notifie au responsable du traitement toute violation de données à caractère personnel dans les meilleurs délais après en avoir pris connaissance.
3. La notification visée au paragraphe 1 doit, à tout le moins :
a) décrire la nature de la violation de données à caractère personnel y compris, si possible, les catégories et le nombre approximatif de personnes concernées par la violation et les catégories et le nombre approximatif d'enregistrements de données à caractère personnel concernés ;
b) le nom et les coordonnées du délégué à la protection des données ou d'un autre point de contact auprès duquel des informations supplémentaires peuvent être obtenues ;

c) décrire les conséquences probables de la violation de données à caractère personnel ;
d) décrire les mesures prises ou que le responsable du traitement propose de prendre pour remédier à la violation de données à caractère personnel, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives.
4. Si, et dans la mesure où, il n'est pas possible de fournir toutes les informations en même temps, les informations peuvent être communiquées de manière échelonnée sans autre retard indu.
5. Le responsable du traitement documente toute violation de données à caractère personnel, en indiquant les faits concernant la violation des données à caractère personnel, ses effets et les mesures prises pour y remédier. La documentation ainsi constituée permet à l'autorité de contrôle de vérifier le respect du présent article."

Article 34 du RGPD

"1. Lorsqu'une violation de données à caractère personnel est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne physique, le responsable du traitement communique la violation de données à caractère personnel à la personne concernée dans les meilleurs délais.
2. La communication à la personne concernée visée au paragraphe 1 du présent article décrit, en des termes clairs et simples, la nature de la violation de données à caractère personnel et contient au moins les informations et mesures visées à l'article 33, paragraphe 3, points b), c) et d).
3. La communication à la personne concernée visée au paragraphe 1 n'est pas nécessaire si l'une ou l'autre des conditions suivantes est remplie :
a) le responsable du traitement a mis en œuvre les mesures de protection techniques et organisationnelles appropriées et ces mesures ont été appliquées aux données à caractère personnel affectées par ladite violation, en particulier les mesures qui rendent les données à caractère personnel incompréhensibles pour toute personne qui n'est pas autorisée à y avoir accès, telles que le chiffrement ;
b) le responsable du traitement a pris des mesures ultérieures qui garantissent que le risque élevé pour les droits et libertés des personnes concernées visé au paragraphe 1 n'est plus susceptible de se matérialiser ;
c) la communication exigerait des efforts disproportionnés. Dans ce cas, il est plutôt procédé à une communication publique ou à une mesure similaire permettant aux personnes concernées d'être informées de manière tout aussi efficace
4. Si le responsable du traitement n'a pas déjà communiqué à la personne concernée la violation de données à caractère personnel la concernant, l'autorité de contrôle peut, après avoir examiné si cette violation de données à caractère personnel est susceptible d'engendrer un risque élevé, exiger du responsable du traitement qu'il procède à cette communication ou décider que l'une ou l'autre des conditions visées au paragraphe 3 est remplie".

3. Motivation

3.1. En ce qui concerne les constatations relatives à la responsabilité du défendeur (articles 5, 24, 32, 33 et 34 du RGPD)

Constatations du rapport d'inspection

19. Dans son rapport d'inspection, le Service d'Inspection constate que le défendeur "*ne donne aucune justification sur la manière dont il parvient à une approche concrète basée sur les risques telle qu'imposée (notamment) par les articles 5, 24, 32, 33 et 34 du RGPD. Les renvois du [défendeur] à la "méthode ENISA pour les fuites de données" et à la "méthode de la CNIL pour une AIPD" sont de nature très générale et vagues ; le [défendeur] n'a pas agi dans ce dossier conformément à l'article 5, deuxième alinéa et à l'article 24, premier alinéa du RGPD*'. [Tous les passages cités dans la présente décision ont été traduits librement par le Secrétariat de l'Autorité de protection des données, en l'absence de traduction officielle].".

Moyens de défense du défendeur

20. En ce qui concerne ce constat du Service d'Inspection, le défendeur affirme qu'il déduit de la lecture conjointe des dispositions précitées que cette prévention concerne premièrement l'obligation de réaliser une analyse d'impact relative à la protection des données au sens de l'article 35 du RGPD et il argumente que selon lui, pour le traitement en question, il n'était pas obligé de procéder à une telle analyse ni à une quelconque autre évaluation des risques.

21. À cet égard, il affirme premièrement que l'acte qui a donné lieu à la fuite de données a eu lieu *avant* la date d'application du RGPD et dès lors de l'article 35 du RGPD, qui introduit le concept d'analyse d'impact relative à la protection des données.

22. Deuxièmement, le défendeur souligne que l'obligation de réaliser une telle analyse d'impact ne s'applique que lorsque le traitement est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques. Il affirme qu'en l'espèce, l'activité de traitement réalisée par le sous-traitant et qui était à l'origine de la fuite de données avait toutefois été expressément interdite par le défendeur. Le défendeur précise que pour tester et développer le logiciel, le sous-traitant a utilisé un environnement de non-production dans lequel il pouvait uniquement utiliser des données anonymisées. Le défendeur en conclut dès lors qu'on ne pouvait pas attendre de lui qu'il réalise une analyse d'impact concernant une activité de son sous-traitant dont il ignorait l'existence et pour laquelle il avait interdit contractuellement l'utilisation de données à caractère personnel.

Le défendeur renvoie à cet égard à l'Annexe C035A2 intitulée "*Data Privacy Requirements*", jointe au *Master IT Service Agreement* conclu en 2014 entre les parties, qui contient une clause affirmant que "*les données confidentielles ne peuvent pas être copiées d'un environnement de production vers un environnement qui n'est pas de production, sauf si les données confidentielles sont masquées*". Il se réfère également à l'article 7 du contrat de sous-traitance conclu ultérieurement entre les parties, qui dispose notamment ce qui suit : "Le prestataire est obligé, pour le traitement de données à caractère personnel *(…) :*

r) d'anonymiser les données à caractère personnel dans un environnement de non-production au moyen d'une technologie industrielle standard qui permet toujours le développement, le test et l'acceptation chez les prestataires ou [le défendeur] ".

23. Le défendeur souligne également qu'à la suite de la fuite de données du 15 juin 2018, il a formellement mis le sous-traitant en demeure et il en joint la preuve.

24. Par ailleurs, en ce qui concerne cette partie de la prévention, le défendeur affirme qu'il a bel et bien pris les mesures organisationnelles adéquates afin d'évaluer les risques et de garantir un niveau de protection adéquat afin d'éviter de tels risques. Il affirme que ladite Annexe C035A2 du contrat conclu le 17 juin 2014 avec le sous-traitant contenait un relevé des risques relatifs au traitement de données à caractère personnel, les mécanismes majeurs afin de protéger les données à caractère personnel ainsi que les obligations du sous-traitant à cet égard.

25. Le défendeur indique que conformément à l'article 6.2 de l'annexe précitée, des audits annuels du sous-traitant étaient en outre prévus et il joint les deux derniers rapports d'audit, établis par *Ernst & Young LLP*, à titre de preuve.

26. Enfin, défendeur argumente qu'il dispose bien d'une méthode d'analyse des risques pour les fuites de données, et qu'il en disposait au moment de la fuite de données de 2018 ainsi qu'ultérieurement. Il se réfère à cet égard à sa "*Data Breach Severity Assessment Method",* basée sur la méthode ENISA, complétée notamment par les normes ISO 31000 et ISO 27005 et il joint une documentation à cet égard dans ses conclusions en réponse. Le défendeur affirme qu'en plus de cette méthode d'analyse des risques pour les fuites de données, il dispose également d'une méthode générale d'analyse des risques. Il se réfère à cet égard à sa politique interne "*Security Risk Management Policy*", qui est utilisée pour évaluer les risques inhérents à toutes les activités de traitement. Le défendeur joint à cet égard une documentation ainsi qu'un exemple d'analyse sur la base de cette méthode, datant du 16 septembre 2017.

27. Le défendeur ajoute que sur la base de la méthode d'évaluation précitée, les risques liés à la fuite de données ayant donné lieu à la saisine de ce dossier ont été évalués. Il précise que dans le cadre

de cette procédure, (l'équipe du) délégué à la protection des données, le *security manager* et le *chief compliance officer* ont successivement été impliqués dans cette évaluation des risques, après quoi leur analyse a été approuvée par le comité de direction du défendeur.

28. Le défendeur souligne lors de l'audition que dans ce dossier, tant lui-même que l'Autorité de protection des données en sont arrivés à la conclusion que le risque de la fuite de données devait être considéré comme élevé et que le défendeur avait pris toutes les mesures nécessaires à cet égard[2] et qu'il ne comprend dès lors pas sur quoi repose la prévention relative au non-respect de la responsabilité.

Analyse de la Chambre Contentieuse

29. La Chambre Contentieuse indique que la responsabilité de l'article 5.2 du RGPD constitue un des piliers centraux du RGPD et implique que le responsable du traitement a la responsabilité, d'une part, de prendre des mesures proactives afin de garantir le respect des prescriptions du RGPD et, d'autre part, de pouvoir prouver qu'il a pris de telles mesures.[3]

C'est ce qui ressort notamment de l'Avis 3/2010 relatif au "principe de responsabilité" du Groupe 29, qui affirme que deux aspects doivent être soulignés à l'égard de ce principe :

(i) "*la nécessité pour le responsable du traitement des données de prendre des mesures appropriées et efficaces pour mettre en œuvre les principes de protection des données ; et*

(ii) *la nécessité de démontrer, sur demande, que des mesures appropriées et efficaces ont été prises. En conséquence, le responsable devrait fournir des preuves de l'exécution du point (i) ci-dessus*".[4]

30. Cette responsabilité concerne non seulement les dispositions de l'article 5.1 du RGPD mais aussi l'ensemble du RGPD.

31. Ce qui précède découle de la lecture conjointe de l'article 5.2 et de l'article 24.1 du RGPD disposant 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 des personnes physiques, le responsable du traitement met en œuvre des mesures techniques et organisationnelles*

[2] Notamment la notification et la notification complémentaire à l'Autorité de protection des données, un communiqué de presse et des notifications individuelles à toutes les personnes concernées.

[3] DOCKSEY, C., "Article 24. Responsibility of the controller" in KUNER, C., BYGRAVE, L.A. et DOCKSEY, C. (eds.), *The EU General Data Protection Regulation: A Commentary,* Oxford University Press, 2020, (508)557: "*The principle of accountability is one of the central pillars of the GDPR and one of its most significant innovations. It places responsibility firmly on the controller to take proactive action to ensure compliance and to be ready to demonstrate that compliance*".

[4] Avis 3/2010 sur le principe de la responsabilité adopté le 13 juillet 2010 par le Groupe 29, pp. 9-10, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp173_fr.pdf.

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."

32. La Chambre Contentieuse souligne que la responsabilité appliquée aux fuites de données implique qu'un responsable du traitement a non seulement la responsabilité de notifier les fuites de données le cas échéant à l'autorité de contrôle et aux personnes concernées, conformément aux articles 33 et 34 du RGPD, mais aussi qu'il doit pouvoir démontrer à tout moment qu'il a pris les mesures nécessaires afin de pouvoir respecter cette obligation.[5]

33. Dans son Avis 3/2010, le Groupe 29 reprend une liste non exhaustive de "mesures de responsabilité" que les responsables du traitement peuvent prendre afin de respecter cette obligation. Le Groupe 29 évoque notamment à cet égard : l'instauration de procédures internes, la mise en place de politiques de protection des données écrites et contraignantes, la désignation d'un délégué à la protection des données, l'élaboration de procédures internes pour une gestion et une déclaration efficaces des infractions.[6]

34. En ce qui concerne l'évaluation de l'efficacité de ces mesures, le Groupe 29 renvoie à l'exécution d'audits internes et/ou externes à titre de bonne pratique. Il précise à cet égard que les méthodes de contrôle pour l'évaluation de l'efficacité des mesures prises doivent correspondre aux risques spécifiques qu'entraîne le traitement de données, à la quantité de données à traiter et au caractère sensible de ces données.[7]

35. Enfin, il convient de souligner que la transparence fait partie intégrante de la responsabilité et que cette transparence à l'égard des autorités de contrôle et des personnes concernées ainsi que du grand public place le responsable du traitement en position favorable quant à sa responsabilité.[8]

36. La Chambre Contentieuse estime que sur la base des pièces déposées et de sa défense, le défendeur démontre que conformément à l'article 24.1 du RGPD, il a pris en l'espèce les mesures techniques et organisationnelles et que conformément à l'article 5.2 du RGPD, il a également démontré, à la demande de l'Autorité de protection des données, qu'il avait pris de telles mesures.

Le défendeur démontre plus précisément :

---

[5] FOCQUET, A. et DECLERCK, E., *Gegevensbescherming in de praktijk*, Intersentia, 2019, 64.

[6] Avis 3/2010 sur le principe de la responsabilité adopté le 13 juillet 2010 par le Groupe 29, pp. 12-13, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp173_fr.pdf

[7] Idem, p. 16-17.

[8] Idem, p. 16.

- que dans ses contrats avec le sous-traitant - aussi bien dans le *Master IT Service Agreement* conclu en 2014 que dans le contrat de sous-traitance conclu après l'entrée en vigueur du RGPD - , il a repris les dispositions nécessaires afin de réglementer le traitement de données à caractère personnel par le sous-traitant, et plus particulièrement d'interdire le traitement de données à caractère personnel par celui-ci à des fins de développement et de test d'un logiciel (en particulier dans l'Annexe C035A2 jointe au Master IT Service Agreement et à l'article 7 du contrat de sous-traitance conclu le 6 juin 2018) ;

- qu'il a développé et documenté les méthodes internes d'analyse des risques requises, aussi bien en ce qui concerne les fuites de données (la "*Data Breach Severity Assessment Method")* qu'en ce qui concerne l'évaluation de risques inhérents à *toutes* les activités de traitement *("Security Risk Management Policy*") et qu'il a également remis cette documentation à la Chambre Contentieuse, de même qu'un exemple d'application de cette méthode ;

- qu'il évalue l'efficacité des procédures et mesures qu'il a élaborées au moyen d'audits externes annuels ;

- que dès qu'il a été informé de la fuite de données par la CERT, il a agi en toute transparence aussi bien à l'égard de l'Autorité de protection des données que des personnes concernées. Conformément à l'article 33 du RGPD, le défendeur a introduit un formulaire de notification ainsi qu'une notification complémentaire à l'Autorité de protection des données, respectivement les 4 et 6 juin 2018. Conformément à l'article 34 du RGPD, le défendeur a également communiqué la violation de données à caractère personnel aux personnes concernées et a publié à cet égard un communiqué de presse le 15 juin 2018 ; et

- qu'il a mis formellement son sous-traitant en demeure le 15 juin 2018 suite au traitement interdit et qu'il en fournit la preuve.

37. La Chambre Contentieuse estime dès lors que l'on ne peut constater **aucune violation des articles 5.1 f), 5.2, 24.1, 32, 33, 34 et 35 du RGPD**.

3.2. <u>En ce qui concerne les constatations relatives à l'obligation de conclure un contrat avec les sous-traitants (article 28 du RGPD)</u>

<u>*Constatations du rapport d'inspection*</u>

38. Dans le rapport d'inspection transmis par le Service d'Inspection à la Chambre Contentieuse le 12 août 2019, on établit que le défendeur "*au moment de la violation de données à caractère personnel*

(au cours de la période comprise entre le 22/03/2018 et le 28/05/2018), n'avait pas conclu de contrat avec le sous-traitant pour l'activité de traitement en question. Le contrat n'a été conclu par [le défendeur] que le 06/06/2018, comme en atteste la date au-dessus de la signature de la personne qui a signé au nom [du défendeur]. Dès lors, dans ce dossier, [le défendeur] n'a pas agi conformément à l'article 28 du RGPD'.".

Moyens de défense du défendeur

39. Dans ses conclusions en réponse et lors de l'audition, le défendeur affirme en réponse à cette prévention que le 17 juin 2014, un contrat global "*Master IT Service Agreement*" a été conclu et que ce contrat fixait expressément les obligations en matière de protection des données à caractère personnel en son article 14.4. Le défendeur ajoute que l'Annexe C035A2 intitulée "*Data Privacy Requirements*", faisant partie intégrante du *Master IT Service Agreement*, contenait des obligations complémentaires pour le sous-traitant.[9]

40. Lors de l'audition du 8 avril 2020, le défendeur souligne que le contrat conclu le 17 juin 2014 avec le sous-traitant, et plus particulièrement son article 14.4, répondait aux conditions imposées par la loi de 1992[10], qui disposait notamment qu'un contrat devait être établi entre les parties et qu'il devait prévoir que le sous-traitant ne traite des données à caractère personnel que sur instruction du responsable du traitement et non pour d'autres finalités que celles définies par ce dernier.

41. Le défendeur ajoute que cette clause était déjà toutefois bien plus large car elle contenait également des dispositions sur les fuites de données et l'assistance et qu'elle contenait ainsi déjà plusieurs éléments qui ont ensuite été imposés par le RGPD.

42. Par ailleurs, le défendeur affirme que lors de l'entrée en vigueur du RGPD, des négociations ont eu lieu avec le sous-traitant et un nouveau contrat de sous-traitance a été établi, lequel a été signé le 21 mai 2018 par le sous-traitant et le 6 juin 2018 par le défendeur lui-même. Le défendeur affirme que la signature de ce contrat par le dernier cité ne constituait qu'une formalité et que le fait qu'elle n'ait eu lieu que le 6 juin 2018 n'est pas pertinent étant donné que ce contrat ne contient des obligations que pour le sous-traitant.

[9] Conclusion en réponse du défendeur n° 57, p. 15.

[10] Loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel (abrogée).

Analyse de la Chambre Contentieuse

43. Conformément à l'article 28.3 du RGPD, le traitement par un sous-traitant doit être régi "*par un contrat ou un autre acte juridique au titre du droit de l'Union ou du droit d'un État membre, qui lie le sous-traitant à l'égard du responsable du traitement, définit l'objet et la durée du traitement, la nature et la finalité du traitement, le type de données à caractère personnel et les catégories de personnes concernées, et les obligations et les droits du responsable du traitement.*"Cet article énonce également les mentions obligatoires qu'un tel acte juridique doit contenir[11].

44. La Chambre Contentieuse constate que le contrat de sous-traitance établi par le défendeur lors de l'entrée en vigueur du RGPD contient les mentions obligatoires de l'article 28 du RGPD, mais que celui-ci n'était pas signé par le défendeur à la date d'entrée en vigueur du RGPD.

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

46. Étant donné que le RGPD est devenu applicable à partir du 25 mai 2018, le contrat de sous-traitance conclu entre le défendeur et son sous-traitant devait dès lors être signé au plus tard à cette date par les deux parties.

47. La Chambre Contentieuse constate toutefois qu'il y avait une entente entre les parties au sujet de ce contrat de sous-traitance et que celui-ci avait été établi par le défendeur avant la date d'entrée en vigueur du RGPD et qu'il avait été signé par le sous-traitant.

48. La Chambre Contentieuse estime dès lors que l'on ne doit constater en l'espèce aucune **violation de l'article 28 du RGPD**.

4. Publication de la décision

49. Vu l'importance de la transparence concernant le processus décisionnel de la Chambre Contentieuse, la présente décision est publiée sur le site Internet de l'Autorité de protection des données, conformément à l'article 95, § 1, 8° de la LCA. Toutefois, il n'est pas nécessaire qu'à cette fin, les données d'identification du défendeur soient directement mentionnées.

[11] Article 28.3, a) - h) du RGPD.

PAR CES MOTIFS,

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

- d'ordonner le **non-lieu**, en vertu de l'**article 100, § 1er, 2° de la LCA** ;

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

(sé.) Hielke Hijmans
Président de la Chambre Contentieuse