Autorité de protection des données
Gegevensbeschermingsautoriteit

Chambre Contentieuse

Décision quant au fond 183/2022 du 14 décembre 2022

Numéro de dossier : DOS-2022-00365

Objet : Communication de données à caractère personnel à des tiers sans le consentement de la personne concernée

La Chambre Contentieuse de l'Autorité de protection des données, composée 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 "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 : Madame X, ci-après "la plaignante" ;

La défenderesse : Y, représentée par Me Heidi Waem et Me Simon Verschaeve, dont les bureaux se situent à 1000 Bruxelles, rue aux Laines 70, ci-après “la défenderesse”.

I. Faits et procédure

1. Le 19 janvier 2022, la plaignante introduit une plainte auprès de l'Autorité de protection des données contre la défenderesse.

   La plaignante a sollicité les services de la défenderesse - auprès de laquelle elle avait souscrit une assurance protection juridique - pour le règlement juridique d'un accident de la circulation dont elle avait été victime. Dans le cadre du règlement de ce sinistre, la plaignante a désigné un avocat. Une correspondance a été échangée entre la défenderesse et l'avocat de la plaignante dans le cadre d'un litige concernant la demande d'intervention de la défenderesse par la plaignante dans les honoraires et autres frais occasionnés par cette assistance juridique.

   Suite à une erreur humaine, un collaborateur a envoyé un e-mail concernant cette assistance à une adresse e-mail incorrecte le 2 juin 2021. Cet e-mail contenait les données suivantes : le nom et le prénom de la plaignante, l'avocat de la plaignante, le numéro du dossier, les acomptes versés, le fait que la personne concernée a eu un accident ayant entraîné des lésions, le déroulement du dossier et le litige quant à l'intervention ou non de Y en tant qu'assureur de protection juridique. L'e-mail ne comportait pas d'annexes.

   Le vendredi 4 juin 2021, le DPO de la défenderesse a été contacté par le collaborateur impliqué dans l'incident et une enquête interne a immédiatement été ouverte. Le lundi 7 juin 2021 à 14h58, les informations nécessaires pour déterminer de manière adéquate la nature de l'incident ont été obtenues, après quoi l'enquête interne a été clôturée par le service compétent (Data Protection Unit) à 15h38. La notification à l'APD a eu lieu le même jour à 21h17.

   La défenderesse a également contacté le mauvais destinataire le lundi 7 juin 2021, en lui demandant de détruire l'e-mail et de ne pas partager les informations avec des tiers, les transmettre, les stocker ou les utiliser de quelque manière que ce soit.

   La plaignante a ensuite été informée, le mardi 8 juin 2021, qu'une fuite de données s'était produite. Enfin, la défenderesse a également contacté l'avocat de la plaignante le 9 juin 2021.

2. Le 14 février 2022, la plainte est déclarée recevable par le Service de Première Ligne sur la base des articles 58 et 60 de la LCA et la plainte est transmise à la Chambre Contentieuse en vertu de l'article 62, § 1er de la LCA.

3. Le 11 mars 2022, conformément à l'article 96, § 1er de la LCA, la demande de la Chambre Contentieuse de procéder à une enquête est transmise au Service d'Inspection, de même que la plainte et l'inventaire des pièces.

4. Le 14 avril 2022, l'enquête du Service d'Inspection est clôturée, le rapport est joint au dossier et celui-ci est transmis par l'Inspecteur général au président de la Chambre Contentieuse (article 91, § 1er et § 2 de la LCA).

   Le rapport comporte des constatations relatives à l'objet de la plainte et conclut à :

   1. une violation de l'article 5, paragraphe 1, a) c) et f) et paragraphe 2, de l'article 6, paragraphe 1, de l'article 24, paragraphe 1 et de l'article 25, paragraphes 1 et 2 du RGPD dans le cadre de la plainte dans ce dossier ;
   2. l'absence d'infraction de manière générale à l'article 5, article 24, paragraphe 1 et article 25, paragraphes 1 et 2 du RGPD ;
   3. une violation des articles 33 et 34 du RGPD.

   Le rapport comporte également des constatations qui dépassent l'objet de la plainte. Le Service d'Inspection constate, dans les grandes lignes, que :

   4. il n'y a pas de violation de l'article 38, paragraphe 1, ni de l'article 39 du RGPD ;

5. Le 29 avril 2022, 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.

6. Le 29 avril 2022, les parties concernées sont informées par envoi recommandé des dispositions telles que reprises à l'article 95, § 2 ainsi qu'à l'article 98 de la LCA. Les parties concernées sont également informées, en vertu de l'article 99 de la LCA, des délais pour transmettre leurs conclusions.

   Pour les constatations relatives à l'objet de la plainte, la date limite pour la réception des conclusions en réponse de la défenderesse a été fixée au 10 juin 2022, celle pour les conclusions en réplique de la plaignante au 1er juillet 2022 et enfin celle pour les conclusions en réplique de la défenderesse au 22 juillet 2022.

7. Le 29 avril 2022, la plaignante accepte toutes communications relatives à l'affaire par voie électronique.

8. Le 29 avril 2022, la défenderesse accepte toutes communications relatives à l'affaire par voie électronique.

9. Le 20 mai 2022, la défenderesse demande une copie du dossier (art. 95, § 2, 3° de la LCA), qui lui a été transmise le 23 mai 2022.

10. Le 10 juin 2022, la Chambre Contentieuse reçoit les conclusions en réponse de la défenderesse concernant les constatations relatives à l'objet de la plainte. Ces conclusions comportent également la réaction de la défenderesse concernant les constatations effectuées par le Service d'Inspection en dehors du cadre de la plainte. À titre principal, la défenderesse fait valoir que la procédure et ses modalités d'exécution par le Service

d'Inspection et la Chambre Contentieuse violent les principes généraux de bonne administration. À titre subsidiaire, la défenderesse soutient que cette violation concernant des données à caractère personnel ne constitue pas une violation des principes de licéité, de minimisation des données, de l'intégrité et de la confidentialité du RGPD. Par ailleurs, la défenderesse n'a pas violé le RGPD suite à la notification de la fuite de données à l'APD et à la personne concernée.

11. Le 14 juillet 2022, la Chambre Contentieuse confirme à la défenderesse que la plaignante n'a pas introduit de conclusions en réplique en ce qui concerne les constatations relatives à l'objet de la plainte.

12. Le 20 juillet 2022, la Chambre Contentieuse reçoit la notification de la défenderesse selon laquelle celle-ci n'introduira pas de conclusions en réplique.

II. Motivation

II.1. Principes de bonne administration

13. La défenderesse fait valoir que tant la procédure que ses modalités d'exécution par le Service d'Inspection et la Chambre Contentieuse violent les principes de bonne administration. La défenderesse soutient que par la manière dont la plainte a été examinée, le Service d'Inspection et la Chambre Contentieuse ont violé le principe de précaution. La Chambre Contentieuse l'aurait fait notamment en décidant qu'une enquête du Service d'Inspection était requise dans cette affaire. Le Service d'Inspection aurait violé ces principes en décidant d'étendre le champ d'application de l'enquête au-delà de l'objet de la plainte. La défenderesse affirme également que les principes de caractère raisonnable et de proportionnalité ont été violés. Cette extension susmentionnée du champ d'application portait sur des aspects qui avaient déjà été remis en question et examinés récemment dans le cadre d'une autre enquête du Service d'Inspection et pour lesquels le Service d'Inspection n'avait constaté aucune violation.

14. À cet égard, la Chambre Contentieuse observe qu'elle a effectivement décidé de saisir le Service d'Inspection afin d'effectuer une enquête sur la base de l'article 94, 1° de la LCA. La Chambre Contentieuse évalue dans chaque dossier à la fois les conséquences personnelles potentielles pour un plaignant et les conséquences sociales du traitement litigieux.

La présente affaire concerne une violation en lien avec des données à caractère personnel (fuite de données). Les violations de données à caractère personnel constituent un problème en soi, mais peuvent également être symptomatiques d'un système de sécurité des données vulnérable, voire obsolète. En outre, ces violations peuvent indiquer des faiblesses dans le système, auxquelles il convient de remédier si nécessaire.

15. La Chambre Contentieuse rappelle qu'une plainte donne rarement une image complète ou objective d'un traitement ou d'une situation dénoncée par le plaignant. Vu que la Chambre Contentieuse ne disposait pas de toutes les informations sur les faits pertinents sur la base de la plainte, elle a demandé une enquête au Service d'Inspection. Dans ce contexte, la Chambre Contentieuse souligne qu'une inspection n'est donc pas toujours demandée dans l'intention d'établir nécessairement une violation, mais plutôt pour obtenir un aperçu aussi précis que possible des faits objectifs pertinents. L'enquête du Service d'Inspection peut tout aussi bien exclure une violation que la constater. L'enquête est donc menée à charge et à décharge.

16. La défenderesse fait valoir qu'il ressort clairement de la plainte elle-même que la violation de données à caractère personnel est le résultat d'une erreur humaine, ce qui ressort également rétrospectivement du rapport d'inspection. Bien qu'il ressorte du rapport d'inspection que la violation de données à caractère personnel est en effet dans ce cas la conséquence d'une erreur humaine, la Chambre Contentieuse souligne qu'elle n'avait pas pu l'établir avec une totale certitude au préalable et qu'il ne peut lui être reproché d'avoir ainsi demandé une enquête afin d'obtenir un aperçu complet et précis des circonstances dans lesquelles la violation de données personnelles s'est produite. Plus généralement, la Chambre Contentieuse souligne que la décision sur le suivi d'un dossier conformément à l'article 95, § 1er de la LCA constitue une étape intermédiaire nécessaire dans cette procédure que la Chambre Contentieuse doit pouvoir prendre en toute liberté.

17. La défenderesse fait également valoir que la Chambre Contentieuse aurait dû classer la plainte sans suite sur la base de sa politique de classement sans suite, en particulier le motif de classement sans suite B.3 "Votre plainte est accessoire à un litige plus large qui nécessite d'être débattu devant les cours et tribunaux judiciaires et administratifs ou une autre autorité compétente". Dans ce cadre, la Chambre Contentieuse rappelle qu'elle n'est pas obligée de classer ces plaintes sans suite mais qu'elle jouit du pouvoir discrétionnaire d'examiner individuellement pour chaque plainte si elle la classera sans suite ou non. Dans la présente affaire, il a été décidé de ne pas classer cette plainte sans suite mais la Chambre Contentieuse a décidé de saisir le Service d'Inspection pour les motifs suivants. En sa qualité d'assureur de protection juridique, la défenderesse traite des données sensibles des personnes concernées. La défenderesse traite en outre ces données à grande échelle. Il est donc important que des garanties suffisantes, comme par exemple en matière de confidentialité, soient fournies par la défenderesse afin que ces traitements à grande échelle de données à caractère personnel sensibles soient effectués dans le respect des principes fondamentaux du RGPD.

18. La Chambre Contentieuse souhaite clarifier davantage ce point, sans préjuger de l'analyse des faits sous-jacents à la plainte et des éventuelles violations du RGPD qui pourraient en

découler. La Chambre Contentieuse se réfère à cette fin à l'article 100 de la LCA[1], où sa compétence décisionnelle est définie dans le cadre d'une procédure sur le fond. Cette disposition prévoit explicitement qu'outre une série d'autres mesures, la Chambre Contentieuse a la possibilité de classer une plainte sans suite (article 100, § 1er, 1° de la LCA), également dans la procédure sur le fond. La Chambre Contentieuse souligne qu'il lui est loisible, même dans cette phase, de classer des plaintes sans suite pour des motifs techniques ou des motifs d'opportunité, conformément aux conditions reprises dans la jurisprudence de la Cour des marchés.[2]

19. La défenderesse fait également valoir que le Service d'Inspection a violé le devoir de diligence en décidant d'élargir davantage la portée de l'enquête. Cette extension du champ d'application portait même en outre sur des aspects qui avaient déjà été remis en question et examinés récemment dans le cadre d'une autre enquête du Service d'Inspection et pour lesquels le Service d'Inspection n'avait constaté aucune violation. La défenderesse affirme que pour ces mêmes raisons, les principes de caractère raisonnable et de proportionnalité ont été violés. En outre, le principe de confiance envers la défenderesse a également été violé. Le principe de confiance ou le principe de sécurité juridique implique en effet que "le droit doit être prévisible et accessible de sorte que le justiciable puisse raisonnablement prévoir les conséquences d'un acte donné au moment où celui-ci est accompli".[3] [Traduction libre effectuée par le Service traduction du Secrétariat général de l'Autorité de protection des données, en l'absence de traduction officielle] En outre, l'autorité publique ne peut pas s'écarter d'une ligne politique sans justification objective et raisonnable, selon la défenderesse.[4] La défenderesse soutient en outre que le principe d'égalité et le principe de non-discrimination tels que repris aux articles 10 et 11 de la Constitution ont également été violés. En effet, on ne peut raisonnablement justifier pourquoi l'APD donne suite à la fuite de

---

[1] Art. 100. § 1er. La chambre contentieuse a le pouvoir de:
1° classer la plainte sans suite ;
2° ordonner le non-lieu ;
3° prononcer la suspension du prononcé ;
4° proposer une transaction ;
5° formuler des avertissements et des réprimandes ;
6° ordonner de se conformer aux demandes de la personne concernée d'exercer 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 État ou un organisme international ;
15° transmettre le dossier au parquet du Procureur du Roi de Bruxelles, qui l'informe des suites données au dossier.

[2] Arrêt de la Cour des marchés du 2 septembre 2020, 9.4.

[3] I. OPDEBEEK et S. DE SOMER, « Hoofdstuk III - Beginselen van behoorlijk bestuur » dans S. DE SOMER et I. OPDEBEEK (ed.), Algemeen bestuursrecht (deuxième édition) - édition reliée, 2e édition, Bruxelles, Intersentia, 2019, p. 412-413.

[4] I. OPDEBEEK et S. DE SOMER, « Hoofdstuk III - Beginselen van behoorlijk bestuur » dans S. DE SOMER et I. OPDEBEEK (ed.), Algemeen bestuursrecht (deuxième édition) - édition reliée, 2e édition, Bruxelles, Intersentia, 2019, p. 412-413.

données dans le cas présent, alors que des fuites de données similaires par des tiers ne font l'objet d'aucune suite. Le fait que, selon ses critères d'évaluation, le Secrétariat général ait apparemment décidé dans un premier temps qu'aucun suivi n'était nécessaire et que la notification de la fuite de données n'ait fait l'objet d'un suivi que plusieurs mois plus tard, à l'initiative du Service d'Inspection, montre également que dans le cas présent, à constellations de faits égales, il ne peut être question d'égalité de traitement.

20. À cet égard, la Chambre Contentieuse se réfère à l'article 72 de la LCA, selon lequel l'Inspecteur général et les inspecteurs "*peuvent procéder à toute enquête, tout contrôle et toute audition, ainsi que recueillir toute information qu'ils estiment utile afin de s'assurer que les principes fondamentaux de la protection des données à caractère personnel, dans le cadre de la présente loi et des lois contenant des dispositions relatives à la protection du traitement des données à caractère personnel, sont effectivement respectées*".

21. Compte tenu de ce qui précède, il appartient au Service d'Inspection, dans le cadre des pouvoirs qui lui sont conférés, de prendre toute mesure d'enquête qu'il juge nécessaire. La Chambre Contentieuse elle-même, en tant qu'organe contentieux administratif, doit fonder ses décisions sur des actes d'enquête qui relèvent clairement du cadre juridique au sein duquel les organes administratifs doivent agir.[5] Dans la présente affaire, il n'y a aucune raison de remettre en cause la licéité des actes d'enquête du Service d'Inspection.

II.2. Article 5, paragraphe 1, a), c) et f) et paragraphe 2, article 6, paragraphe 1, article 24, paragraphe 1 et article 25, paragraphes 1 et 2 du RGPD

22. En sa qualité de responsable du traitement, la défenderesse est tenue de respecter les principes de protection des données et doit être en mesure de démontrer que ceux-ci sont respectés (principe de responsabilité – article 5, paragraphe 2 du RGPD).

23. Elle doit en outre, également en sa qualité de responsable du traitement, prendre toutes les mesures nécessaires pour garantir et pouvoir démontrer que le traitement est réalisé conformément au RGPD (articles 24 et 25 du RGPD).

24. La Chambre Contentieuse rappelle le principe de l'article 5, paragraphe 1, a) du RGPD qui prévoit que les données à caractère personnel ne peuvent être traitées que de manière licite. Cela signifie qu'il doit y avoir une base juridique pour le traitement de données à caractère personnel, telle que visée à l'article 6, paragraphe 1 du RGPD. Pour étoffer ce principe de

[5] par analogie avec l'arrêt de la cour d'Appel de Bruxelles (Cour des marchés) du 7 juillet 2021, p. 18 : "Dans le cadre de compétences discrétionnaires, les principes de bonne administration permettent au juge d'examiner si l'administration a exercé le pouvoir qui lui est conféré dans les limites de la légalité. À cet égard, le juge n'a qu'un droit de contrôle marginal. Le juge ne peut déclarer le comportement dénoncé comme fautif que s'il va à l'encontre des opinions de tout organe administratif normalement prudent et raisonnable. Tel est le cas notamment lorsque la décision ne serait pas fondée sur des données concrètes et irait à l'encontre du caractère raisonnable, et que l'administration commettrait par conséquent une erreur manifeste d'appréciation. Le principe de "raisonnabilité" ne limite le pouvoir discrétionnaire qu'en ne tolérant pas que ce qui a été décidé soit manifestement disproportionné par rapport aux faits (y compris toutes les pièces du dossier) sur lesquels la décision est fondée. [Traduction libre effectuée par le service traduction de l'Autorité de protection des données, en l'absence de traduction officielle]

base, l'article 6, paragraphe 1 du RGPD prévoit que les données à caractère personnel ne peuvent être traitées qu'en vertu d'une des bases juridiques énoncées dans cet article. Lorsque des données à caractère personnel sont traitées, elles doivent donc être adéquates et pertinentes au regard de la finalité. Par ailleurs, on ne peut pas traiter plus de données à caractère personnel que ce qui est nécessaire au regard de la finalité (article 5.1.c) du RGPD). L'article 5.1.f) du RGPD prescrit que les données à caractère personnel doivent être "*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*".

25. En ce qui concerne le traitement litigieux, le Service d'Inspection constate dans son rapport que dans le cadre de la plainte dans le présent dossier, la défenderesse a commis une violation de l'article 5, paragraphe 1, a), c), f) et paragraphe 2 du RGPD, sur la base des éléments suivants :

- le principe de licéité a été violé car l'envoi de données à caractère personnel de la plaignante à un mauvais destinataire ne reposait pas sur une base juridique telle que reprise à l'article 6, paragraphe 1 du RGPD ;
- le principe de minimisation des données a été violé car la défenderesse a traité davantage de données à caractère personnel de la plaignante que ce qui était nécessaire suite à leur envoi à un mauvais destinataire ;
- le principe d'intégrité et de confidentialité a été violé car en envoyant des données à caractère personnel de la plaignante à un mauvais destinataire, la défenderesse a compromis la confidentialité de ces données à caractère personne ; et
- en envoyant des données à caractère personnel de la plaignante à un mauvais destinataire, la défenderesse a omis de prendre les mesures techniques et organisationnelles nécessaires pour s'assurer et être en mesure de démontrer que le traitement a été effectué conformément au RGPD.

26. Malgré cette violation des articles précités dans le cadre du présent dossier, le Service d'Inspection constate que la partie défenderesse cherche généralement à respecter les obligations imposées par l'article 5 du RGPD. Le Service d'Inspection observe toutefois que cela n'enlève rien à la violation concrète mentionnée ci-dessus.

27. La défenderesse reconnaît que l'e-mail daté du 2 juin 2021 était adressé à la plaignante, mais qu'en raison d'une erreur humaine ponctuelle, des données à caractère personnel relatives à la plaignante ont été envoyées par inadvertance à un tiers. Elle explique que cela est dû au fait que l'adresse e-mail de l'avocat de la plaignante est similaire à une autre adresse e-mail

dans le système de messagerie de la défenderesse. La défenderesse soutient qu'une telle action involontaire, non intentionnelle, ne peut pas donner lieu à une violation du RGPD.

28. La défenderesse fait valoir qu'elle a pris toutes les mesures appropriées pour se conformer à ses obligations en matière de protection des données. Ainsi, elle a pris les mesures suivantes, qui sont pertinentes dans le cas présent :

    a. Rédaction et déploiement d'une politique de confidentialité et de protection des données dans toute l'entreprise ("Group Compliance Rule Data Protection") qui clarifie les exigences du RGPD et leur mise en œuvre pour les entités du groupe Y ;

    b. Système de classification des e-mails internes et externes (dans les catégories public, internal, confidential et strictly confidential) ;

    c. Mise en place d'un message d'avertissement dans le système de messagerie électronique de la défenderesse lorsque des collaborateurs envoient un e-mail à une adresse e-mail externe ;

    d. Cryptage et protection par mot de passe des pièces jointes aux e-mails externes dont le contenu est (strictement) confidentiel ;

    e. Mesures de contrôle d'accès aux systèmes de la défenderesse ;

    f. Mesures en matière de masquage d'informations dans les systèmes internes de la défenderesse ;

    g. Afin d'informer de manière proactive les départements des questions qu'ils doivent prendre en compte, une "Compliance Checklist" a été déployée avec une section explicite pour la protection des données ;

    h. Rédaction et mise en œuvre d'un "Health Data Framework", qui comprend la politique et la stratégie de la défenderesse en matière de traitement des données relatives à la santé. Ce Health Data Framework est revu annuellement par des représentants de différentes fonctions (à risque) (Compliance (dont le DPO fait partie), Legal, Risk, CC Privacy, politique d'indemnités, communauté médicale, ...). Le Framework fournit des lignes directrices concrètes et définit les exigences pour le traitement des données médicales au sein de Y Assurances, notamment (i) des règles concernant la communication de données relatives à la santé et l'utilisation de canaux de communication sécurisés, tant en interne qu'en externe, (ii) des règles spécifiques concernant le traitement par des tiers, parties externes et (iii) des règles spécifiques concernant la conservation des données relatives à la santé ;

    i. Dans le domaine Information Security, il existe un cadre complet de normes de groupe qui contiennent directement ou indirectement des règles sur la protection

des données et la confidentialité, comme par exemple quels moyens de communication peuvent être utilisés pour quel type de données ;

j. Formation et conscientisation : la défenderesse veille à ce que ses employés sachent comment traiter les données à caractère personnel de manière appropriée et sécurisée. Tous les collaborateurs doivent suivre une formation de base obligatoire sur le RGPD. En outre, la défenderesse a lancé une formation en ligne pour tous ses collaborateurs qui traitent des données relatives à la santé. Cette formation en ligne se concentre plus en détail sur le traitement des données relatives à la santé et comprend des parties importantes telles que des directives claires sur l'utilisation de canaux de communication sécurisés, entre autres. Une mise à jour de cette formation a été effectuée et la nouvelle version a été mise en œuvre le 24 janvier 2022. Les sessions de formation doivent obligatoirement être répétées à intervalles réguliers. La participation à ces formations fait l'objet d'un enregistrement et d'un suivi, et les connaissances acquises sont ensuite vérifiées par un test obligatoire ;

k. Outre les sessions de formation obligatoires, des communications mensuelles sur divers sujets relatifs au RGPD sont publiées via la plateforme de communication interne "Y Connect" ;

l. En plus des procédures de gouvernance interne, plusieurs services de soutien au sein de la défenderesse fournissent quotidiennement conseils et soutien concernant le RGPD, notamment : (i) le Competence Center Privacy central (ci-après "CC Privacy") en première ligne, (ii) soutenu par les Compliance Risk Managers (CORM) nommés de manière décentralisée en première ligne et (iii) la Group Compliance Data Protection Unit, dont le DPO de Y Assurances est membre, en deuxième ligne.

29. La défenderesse fait valoir qu'elle préfère communiquer par des canaux plus sécurisés que les e-mails (comme certaines applications), mais cela n'est pas toujours possible. La présente affaire concerne des communications avec l'avocat d'un client de sorte que l'e-mail était le seul canal de communication électronique disponible pour la défenderesse. Enfin, la défenderesse souligne qu'elle a fait de nombreux efforts pour atténuer ce genre de risques, mais que l'erreur humaine restera toujours un risque résiduel.

30. La Chambre Contentieuse attire l'attention sur le fait que la présence ou non d'une intention ne constitue pas un critère pour la présence ou non d'un traitement de données à caractère personnel au sens de l'article 4, point 2) du RGPD.[6] Bien qu'il n'était pas dans l'intention de la

[6] Article 4 du RGPD : "Aux fins du présent règlement, on entend par :
[...]

défenderesse d'envoyer l'e-mail au tiers, le seul fait que l'e-mail ait bel et bien été envoyé au mauvais destinataire suffit pour qualifier cet envoi de traitement, dont il convient de vérifier la licéité.

31. Comme l'a également reconnu la défenderesse, il est question en l'espèce d'une violation de données à caractère personnel. À toutes fins utiles, la Chambre Contentieuse rappelle qu'une violation de données à caractère personnel est une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données. En envoyant l'e-mail au mauvais destinataire, ce tiers pouvait également accéder à ces données personnelles de la plaignante. Il est dès lors question d'une violation de confidentialité, à savoir une communication ou un accès illicite ou involontaire de/à des données à caractère personnel. Les données à caractère personnel en question ont en effet été exposées involontairement pendant une (courte) période à des personnes externes, mettant ainsi en péril la confidentialité.

32. La Chambre Contentieuse estime que l'ensemble des éléments exposés démontre que la défenderesse ne peut s'appuyer sur aucun fondement juridique de l'article 6, paragraphe 1 du RGPD démontrant la licéité du traitement de données contesté. En outre, le traitement des données a compromis la confidentialité et l'intégrité, vu que des tiers ont pu prendre connaissance de ces données.

33. Pour autant que nécessaire, la Chambre Contentieuse rappelle également qu'en vertu de l'article 9 du RGPD, les données sensibles, telles que les données relatives à la santé (en l'espèce, l'e-mail contenait le fait que la personne concernée avait eu un accident ayant entraîné des lésions), ne peuvent en principe pas être traitées. Compte tenu de leur nature sensible, le traitement des catégories particulières de données à caractère personnel fait donc l'objet d'une interdiction générale de traitement. Le RGPD formule toutefois un nombre limité d'exceptions à cette règle et ces exceptions s'appliquent à toutes les catégories particulières de données personnelles. Par souci d'exhaustivité, la Chambre Contentieuse souligne qu'aucune de ces exceptions ne pouvait être utilisée pour le traitement de données en cause.

34. À cet égard, la Chambre Contentieuse estime que comme l'envoi était une erreur, l'intention n'était pas du tout d'envoyer l'e-mail au mauvais destinataire, et que la défenderesse n'avait pas prévu qu'un tel envoi se produirait. Cela découle en effet de la nature même d'une erreur.

---

2) "traitement" toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction"

Ceci est d'autant plus vrai que, dans le cas d'espèce, il n'existe pas de mesures techniques ou organisationnelles permettant d'exclure complètement le risque qu'un e-mail soit envoyé à un mauvais destinataire en raison d'une erreur humaine.

35. Bien que cette violation de données à caractère personnel constitue une violation des principes fondamentaux de l'article 5, paragraphe 1 et de l'article 6, paragraphe 1 du RGPD, la Chambre Contentieuse constate que la défenderesse a pris les mesures techniques et organisationnelles appropriées nécessaires pour respecter les principes fondamentaux de l'article 5, paragraphe 1 et le démontrer. Il ressort également du rapport d'Inspection que la défenderesse respecte globalement les obligations imposées par les articles 5, 24, paragraphe 1 et 25, paragraphes 1 et 2, du RGPD. En l'espèce, le traitement litigieux concerne une erreur humaine, dont le risque n'est jamais totalement inexistant.

36. Dans une liste non exhaustive de mesures que les responsables du traitement peuvent prendre pour respecter le principe de responsabilité, le Groupe 29 renvoie dans ses Lignes directrices sur la notification de violations de données à caractère personnel en vertu du Règlement 2016/679[7], entre autres, aux mesures suivantes à prendre : la mise en œuvre et la surveillance des procédures de contrôle pour s'assurer que toutes les mesures n'existent pas seulement sur le papier mais sont également exécutées et fonctionnent dans la pratique, l'établissement de procédures internes, l'élaboration d'une politique écrite et contraignante en matière de protection des données, le développement de procédures internes pour la gestion et la notification efficaces de violations de la sécurité. Les documents montrent que la défenderesse mène régulièrement des actions de sensibilisation et que le personnel est également sensibilisé aux principes de base et aux obligations des responsables de traitement découlant du RGPD. De cette manière, le risque résiduel de telles violations de données à caractère personnel est réduit au minimum.

37. Par conséquent, la Chambre Contentieuse estime qu'il est question d'une violation des articles 5, paragraphe 1, a), c) et f) et paragraphe 2, article 6, paragraphe 1, article 24, paragraphe 1 et article 25, paragraphes 1 et 2, mais que cela ne nécessite pas d'imposer une amende ou une mesure correctrice et qu'il est approprié d'ordonner un abandon des poursuites. À cet égard, la Chambre Contentieuse se réfère au fait que la défenderesse a pris les mesures nécessaires pour obtenir du mauvais destinataire la suppression de l'e-mail ainsi qu'au fait que la violation n'est pas la conséquence d'un problème structurel et que des mesures proactives suffisantes sont en place pour garantir le respect du RGPD.

[7] Lignes directrices *sur la notification d'une violation de données à caractère personnel en vertu du règlement (UE) 2016/679*, wp250rev01, Groupe de travail Article 29.

II.3. Article 33 du RGPD et article 34 du RGPD

II.3.1. Article 33 du RGPD

38. Lorsqu'une telle violation de données à caractère personnel se produit, le RGPD impose au responsable du traitement de le notifier à l'autorité de contrôle nationale compétente et, dans certains cas, de communiquer cette violation aux personnes dont les données à caractère personnel sont concernées par cette violation.

39. En ce qui concerne la notification d'une violation de données à caractère personnel à l'autorité de contrôle, la Chambre Contentieuse se réfère à l'article 33 du RGPD qui dispose que "*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.*"

40. Le Service d'Inspection a conclu dans son rapport que la notification de la violation à l'APD et aux personnes concernées n'a pas été faite en temps utile, sur la base des constatations suivantes. La violation s'est produite le 2 juin 2022, la notification interne de la violation des données à caractère personnel par le collaborateur concerné à la Data Protection Unit de la défenderesse a eu lieu le 4 juin 2022. La notification de la violation de données à caractère personnel à l'APD a eu lieu le 7 juin 2022. Cette notification a donc eu lieu plus de 72 heures après la découverte de la violation des données à caractère personnel, ce qui constitue une violation des articles 33 du RGPD, d'après le rapport d'inspection.

41. La défenderesse conteste ces constatations. Elle soutient que la notification à l'APD a eu lieu en temps utile. La défenderesse fait valoir que le rapport ne montre pas que le Service d'Inspection a suffisamment enquêté sur le moment où l'on peut situer le moment de la prise de connaissance. Contrairement au rapport d'inspection, la défenderesse fait valoir que le point de départ de ce délai n'est pas le moment où la violation s'est effectivement produite, mais bien le moment où le responsable du traitement a été informé d'une violation possible et après avoir effectivement constaté qu'il s'agissait d'un incident à notifier. Les Lignes directrices du Groupe de travail "Article 29" sur la notification de violations de données à caractère personnel en vertu du Règlement (UE) 2016/679[8] disposent en effet que "*Le moment exact où un responsable du traitement peut être considéré comme ayant pris "connaissance" d'une violation spécifique dépendra des circonstances de la violation en*

[8] Lignes directrices *sur la notification d'une violation de données à caractère personnel en vertu du règlement (UE) 2016/679*, wp250rev01, Groupe de travail Article 29, p. 11-14.

question".[9] Selon le Groupe de travail "Article 29", un responsable du traitement a pris connaissance "*Après avoir été informé d'une possible violation par un individu, par une organisation médiatique ou par une autre source, ou encore lorsqu'il a lui-même détecté un incident de sécurité, le responsable du traitement peut mener une brève enquête afin de déterminer si une violation s'est effectivement produite.*"[10] En effet, il peut falloir un certain temps pour déterminer si des données à caractère personnel sont effectivement compromises : "*Cette courte période permet au responsable du traitement d'ouvrir une enquête et de recueillir* des preuves et d'autres données pertinentes", selon la défenderesse. Se référant à ces Lignes directrices du Groupe de travail Article 29, la défenderesse affirme que le point de départ du délai de 72 heures mentionné à l'article 33 du RGPD commence en l'occurrence à courir au moment où la défenderesse a pris connaissance du fait que l'incident concernait des données à caractère personnel qui devaient effectivement être notifiées, après que toutes les informations requises concernant l'incident aient été communiquées par le collaborateur concerné au service compétent en interne (Data Protection Unit) (à savoir le 7 juin 2021 à 15 h 38) et après qu'une analyse ait effectivement établi que l'incident devait être notifié.

42. Comme expliqué ci-dessus, la Chambre Contentieuse rappelle que l'article 33 du RGPD prévoit qu'en cas de violation de données à caractère personnel, le responsable du traitement notifie la violation de données à caractère personnel dans les meilleurs délais et, si possible, 72 heures au plus tard après en avoir pris connaissance. Ainsi, le point de départ du calcul du délai de 72 heures commence au moment où la défenderesse, en tant que responsable du traitement, en a pris connaissance.

43. La question se pose ensuite de savoir quand un responsable du traitement peut être considéré comme ayant pris "connaissance" d'une violation.

44. Sur la base de la notification de la violation des données à caractère personnel par la défenderesse à l'APD, la Chambre Contentieuse constate qu'un collaborateur de la défenderesse a envoyé l'e-mail en question au mauvais destinataire le 2 juin 2021 à 17h16. Dans le formulaire de notification, le délégué à la protection des données indique que le collaborateur a découvert cette erreur suite à une réponse automatique du destinataire. Il a ensuite envoyé l'e-mail au bon destinataire le 2 juin 2021 à 17h24. Les deux e-mails ont été joints en annexe au dossier. Dans la notification de la violation de données à caractère personnel à l'APD, le moment où la défenderesse a pris connaissance de la violation de données à caractère personnel est fixé au 2 juin 2021 à 17:24.

---

[9] Lignes directrices *sur la notification d'une violation de données à caractère personnel en vertu du règlement (UE) 2016/679*, wp250rev01, Groupe de travail article 29, p. 12.

[10] Lignes directrices *sur la notification d'une violation de données à caractère personnel en vertu du règlement (UE) 2016/679*, wp250rev01, Groupe de travail Article 29, p. 13.

45. Comme expliqué ci-dessus, la défenderesse fait valoir dans ses conclusions que le délai de 72 heures a seulement commencé à courir lorsque la Data Protection Unit a reçu tous les documents pertinents du collaborateur concerné afin de procéder à une analyse et après qu'elle ait déterminé, à la suite de cette analyse, qu'il s'agissait bien d'un incident à signaler. Dans ce cadre, la Chambre Contentieuse renvoie aux Lignes directrices de l'EDPB 9/2022 sur les notifications de violations de données à caractère personnel. Le European Data Protection Board (ci-après : EDPB)[11] indique qu'un responsable du traitement des données doit être réputé avoir pris "connaissance" lorsqu'il a un degré raisonnable de certitude qu'un incident de sécurité s'est produit et a conduit à la compromission de données à caractère personnel. Cela doit être évalué en tenant compte des circonstances de la violation spécifique. Dans ces Lignes directrices, l'EDPB cite quelques situations pour illustrer quand il y a un degré raisonnable de certitude qu'un incident de sécurité s'est produit, comme par exemple les suivantes : "*Un tiers informe un responsable du traitement qu'il a accidentellement reçu les données à caractère personnel de l'un de ses clients et fournit la preuve de cette divulgation non autorisée. Dès lors que le responsable du traitement a reçu des preuves claires attestant d'une violation de la confidentialité, il ne fait aucun doute qu'il en a pris "connaissance"*".

46. La Chambre Contentieuse estime qu'en l'espèce, l'exemple ci-dessus de l'EDPB est très similaire aux faits de la présente affaire. Étant donné que le mauvais destinataire a informé l'avocat de la plaignante de la violation des données à caractère personnel, lequel a à son tour informé la défenderesse, il y avait donc un degré raisonnable de certitude qu'un tel incident de sécurité s'était produit. L'EDPB reconnaît la possibilité pour un responsable du traitement de mener une brève enquête pour déterminer si une violation s'est effectivement produite. Lors de cette période d'enquête, le responsable du traitement peut ne pas être considéré comme ayant pris "connaissance".[12] Également dans la situation que la défenderesse évoque dans ses conclusions, l'e-mail de l'avocat de la plaignante (et, de surcroît, le fait que le collaborateur a apparemment découvert lui-même cette erreur suite à une réponse automatique du mauvais destinataire) a permis d'obtenir rapidement un degré raisonnable de certitude qu'une violation de données à caractère personnel avait eu lieu, et que la défenderesse en avait donc pris connaissance.

47. Dès que le responsable du traitement a ainsi pris "connaissance" d'un incident de sécurité, une violation à signaler doit être notifiée à l'autorité de contrôle sans retard déraisonnable et, si possible, dans les 72 heures si la violation des données à caractère personnel est susceptible de présenter un risque pour les droits et libertés des personnes physiques.

[11] EDPB Guidelines 9/2022 on personal data breach notification under GDPR, du 10 octobre 2020, à consulter via https://edpb.europa.eu/system/files/2022-10/edpb_guidelines_202209_personal_data_breach_notification_targetedupdate_en.pdf

[12] EDPB Guidelines 9/2022 on personal data breach notification under GDPR, du 10 octobre 2020 , p. 12.

Au cours de cette période, le responsable du traitement doit évaluer ce risque probable pour les personnes afin de déterminer si l'obligation de notification s'applique effectivement et quelle(s) action(s) est (sont) nécessaire(s) pour remédier à la violation.[13]

48. Seule la courte période dont le responsable du traitement a pu avoir besoin pour évaluer si cet incident constituait une fuite de données n'est pas incluse dans le délai de 72 heures (mais étant donné qu'il y avait ici déjà rapidement un degré raisonnable de certitude, cette période aurait donc dû être dans ce cas particulièrement courte ou quasi-inexistante). Cette période de 72 heures vise certes à donner au responsable du traitement le temps d'effectuer une analyse de risques et d'évaluer si une notification doit être faite à l'APD. Contrairement à ce que soutient la défenderesse, cette période pour effectuer cette analyse de risques est bel et bien comprise dans le délai de 72 heures.

49. Cette violation de données à caractère personnel n'a été signalée à la Data Protection Unit par le collaborateur concerné que dans l'après-midi du vendredi 4 juin 2021. Après que la Data Protection Unit ait été avertie, une analyse de risques a été effectuée et il a été décidé de notifier cette violation de données à caractère personnel à l'APD. Cette notification a eu lieu le lundi 7 juin 2021 à 21:17. Comme l'indique également le registre interne des incidents, cette notification a eu lieu en dehors de la période de 72 heures après la prise de connaissance de l'incident (qui peut être située le 2 juin 2021). L'explication mentionnée était que le collaborateur concerné avait informé tardivement le délégué à la protection des données. Suite à cela, et à la demande de la Data Protection Unit de la défenderesse, une nouvelle action de *sensibilisation* a été entreprise à cet égard. Au vu de ce qui précède, la Chambre Contentieuse conclut que la notification tardive de la fuite de données à l'APD constitue une violation de l'article 33 du RGPD. Compte tenu des mesures prises suite à cette fuite de données, la Chambre Contentieuse conclut qu'une réprimande est appropriée. Au vu des circonstances spécifiques de la présente affaire, l'imposition d'une amende ou d'une mesure correctionnelle serait disproportionnée.

II.3.2. Article 34 du RGPD

50. Conformément à l'article 34 du RGPD, le responsable du traitement doit dans certains cas non seulement notifier une violation à l'autorité de contrôle, mais aussi la communiquer aux personnes touchées par celle-ci. C'est le cas lorsqu'il est probable qu'une violation implique un risque élevé pour les droits et libertés des personnes physiques.

51. Le seuil pour la communication d'une violation aux personnes concernées est donc plus élevé que celui pour la communication aux autorités de contrôle et donc toutes les violations

[13] EDPB Guidelines 9/2022 on personal data breach notification under GDPR, du 10 octobre 2020 , p. 12.

qui sont notifiées à l'autorité de contrôle ne doivent pas être communiquées aux personnes concernées.

52. L'article 34 du RGPD dispose que "*[l]orsqu'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 (aux) personne(s) concernée(s) dans les meilleurs délais. La Chambre Contentieuse observe qu'il n'y a pas de délai de 72 heures fixé pour la notification aux personnes concernées. Cette notification doit être effectuée sans délai, car le principal objectif de la notification aux personnes est de leur fournir des informations spécifiques sur les mesures qu'elles doivent prendre pour se protéger.[14]

53. Dans sa notification de la fuite de données à l'APD, la défenderesse a indiqué que la personne concernée serait informée car la perte de contrôle des données à caractère personnel de la personne concernée par une diffusion allant au-delà de ce qui est nécessaire présente un risque élevé pour les droits et libertés de la personne concernée. Comme déjà expliqué ci-avant, la Data Protection Unit a reçu toute la documentation nécessaire du collaborateur concerné le 7 juin 2021 à 15h38. La Data Protection Unit a ensuite pu analyser si la fuite de données impliquait un risque élevé pour les droits et libertés de la plaignante. La plaignante a ensuite été informée de la fuite de données le jour suivant.

54. La Chambre Contentieuse constate que la fuite de données a eu lieu le 2 juin 2021 et que la plaignante n'en a été informée que le 8 juin 2021. Cela vient du fait que le collaborateur concerné n'a pas informé la Data Protection Unit de la fuite de données à temps, ce qui a empêché celle-ci de procéder à une analyse en temps utile de son impact sur les droits et libertés de la plaignante. Vu ce qui précède, la Chambre Contentieuse conclut qu'il y a violation de l'article 34 du RGPD. La Chambre Contentieuse constate à nouveau que la défenderesse a pris des mesures de sensibilisation suite à cette fuite de données et que la Data Protection Unit a effectué l'analyse requise en vertu de l'article 34 du RGPD le lendemain de la réception des documents nécessaires. Par conséquent, la Chambre Contentieuse conclut qu'une réprimande est appropriée, au vu des circonstances concrètes de la présente affaire.

II.4. Article 38, paragraphe 1 et article 39 du RGPD

55. Le RGPD reconnaît que le délégué à la protection des données est une figure clé en ce qui concerne la protection des données à caractère personnel, dont la désignation, la position et les missions sont soumises à des règles. Ces règles aident le responsable du traitement à

[14] Voir également le considérant 86.

remplir ses obligations en vertu du RGPD mais aident aussi le délégué à la protection des données à exercer correctement ses missions.

56. L'article 38, paragraphe 1 du RGPD prescrit que le responsable du traitement veille à ce que le délégué à la protection des données soit associé, d'une manière appropriée et en temps utile, à toutes les questions relatives à la protection des données à caractère personnel. L'implication du délégué à la protection des données doit contribuer à ce qu'il puisse accomplir effectivement les tâches mentionnées à l'article 39 du RGPD.

57. Après enquête, le Service d'Inspection a conclu qu'aucune violation de l'article 38, paragraphe 1 et de l'article 39 du RGPD n'a pu être constatée. Sur la base des pièces du dossier et des conclusions de la défenderesse, la Chambre Contentieuse estime qu'il n'y a aucune raison d'adopter une position différente à cet égard.

III. Publication de la décision

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

PAR CES MOTIFS,

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

- d'ordonner un non-lieu, en vertu de l'article 100, § 2 de la LCA, suite aux violations
  - de l'article 5, paragraphe 1, c) et f) et paragraphe 2, de l'article 6, paragraphe 1, de l'article 24, paragraphe 1 et de l'article 25, paragraphes 1 et 2 du RGPD ;
- de formuler une réprimande, en vertu de l'article 100, § 5 de la LCA, suite à la violation
  - des articles 33 et 34 du RGPD.

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

Un tel recours peut être introduit au moyen d'une requête contradictoire qui doit comporter les mentions énumérées à l'article 1034*ter* du *Code judiciaire*[15]. La requête contradictoire doit être déposée au greffe de la Cour des marchés conformément à l'article 1034*quinquies* du *Code judiciaire*, ou via le système informatique e-Deposit de la Justice (article 32[16]*ter* du *Code judiciaire*).

(sé.) Hielke HIJMANS

Président de la Chambre Contentieuse

[15] La requête contient à peine de nullité :

1° l'indication des jour, mois et an ;
2° les nom, prénom, domicile du requérant, ainsi que, le cas échéant, ses qualités et son numéro de registre national ou numéro d'entreprise ;
3° les nom, prénom, domicile et, le cas échéant, la qualité de la personne à convoquer ;
4° l'objet et l'exposé sommaire des moyens de la demande ;
5° l'indication du juge qui est saisi de la demande ;
6° la signature du requérant ou de son avocat.

[16] La requête, accompagnée de son annexe, est envoyée, en autant d'exemplaires qu'il y a de parties en cause, par lettre recommandée au greffier de la juridiction ou déposée au greffe.