Autorité de protection des données
Gegevensbeschermingsautoriteit

Chambre Contentieuse

Décision quant au fond 114/2024 du 6 septembre 2024

Numéro de dossier : DOS-2022-00896

Objet : Enregistrement du temps de travail via des données biométriques

La Chambre Contentieuse de l'Autorité de protection des données, composée de Monsieur Hielke Hijmans, président, et de Messieurs Dirk Van Der Kelen et Jelle Stassijns, membres ;

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

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

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

Vu les pièces du dossier ;

A pris la décision suivante concernant :

Le plaignant : X, représenté par Me Gert Buelens, dont le cabinet se situe à 2800 Mechelen, Nekkerspoelstraat 97, ci-après “le plaignant”;

Les défenderesses : Y1, représentée par Me Bernard Dewit, dont le cabinet se situe à 1050 Bruxelles, Place Albert Leemans 20, ci-après “la première défenderesse” ;

Y2, représentée par Me Jos De Wachter et Me Charlotte Peeters, dont le cabinet se situe à 3600 Genk, Jaarbeurslaan 19, boîte 3, ci-après “la deuxième défenderesse” ;
dénommées conjointement "les défenderesses".

I. Faits et procédure

1. Le 3 février 2022, le plaignant a porté plainte auprès de l'Autorité de protection des données contre la première défenderesse. Dans un premier temps, cette plainte n'était pas recevable. La plainte a été réintroduite et déclarée recevable le 29 mars 2022.

   Le plaignant a travaillé auprès de la première défenderesse de mars 2021 au 24 février 2022 inclus, d'abord en tant qu'intérimaire et à partir de juin 2021, comme travailleur avec un contrat à durée indéterminée. Le 16 mars 2020, la première défenderesse a mis en place sur ses deux sites pour tous les membres du personnel y travaillant un système d'enregistrement du temps par empreintes digitales. Selon la première défenderesse, le système s'applique ainsi à quelque 200 travailleurs, dont 44 employés, 74 ouvriers, 29 intérimaires et, pour le reste, des "travailleurs étrangers". Le fournisseur du système (la deuxième défenderesse) est une filiale d'un groupe international ayant son siège au Japon et des activités entre autres aux États-Unis et en Chine. Le plaignant estime que le traitement de ses empreintes digitales (une de chaque main) viole son droit à la protection des données à caractère personnel parce qu'il n'a pas fourni volontairement ces empreintes digitales et parce qu'il n'a pas été informé des modalités de conservation des données ni du délai de conservation. Enfin, le plaignant s'inquiète également dans sa plainte d'un éventuel transfert vers un pays tiers n'offrant pas de garanties suffisantes, compte tenu de la situation géographique du siège de la société mère de la première défenderesse.

2. Le 29 mars 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 21 avril 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 29 août 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 formule les constatations suivantes dans le chef de la première défenderesse :

   1. une violation des articles 5.1.a), 6.1 et 9.1 du RGPD ;
   2. une violation de l'article 5.1.b) du RGPD ;
   3. pas de violation de l'article 5.1.c) du RGPD ;
   4. une violation des articles 5.1.a) *j°* 12.1 et 13 du RGPD ;

5. une violation des articles 5.1.a) *j°* 12.1 et 15 du RGPD ;
6. une violation de l'article 5.2 du RGPD ;
7. une violation de l'article 28.3 du RGPD ;
8. une violation de l'article 28.1 du RGPD ;
9. une violation de l'article 32 du RGPD ;
10. une violation de l'article 35 du RGPD ;
11. aucune indication de transferts éventuels de données biométriques vers des pays tiers ou des organisations internationales.

Le rapport comporte des constatations relatives à l'objet de la plainte dans le chef de la deuxième défenderesse et établit que celle-ci n'a pas respecté son obligation en vertu de l'article 28.3 du RGPD de conclure un contrat de sous-traitance valable.

Le rapport comporte en outre des constatations qui dépassent l'objet de la plainte. Le Service d'Inspection constate, dans les grandes lignes, qu'il est question :

1. d'une violation de l'article 30 du RGPD dans le chef de la première défenderesse pour ne pas avoir tenu de registre des activités de traitement préalablement à l'enquête d'inspection et en raison du contenu incomplet de l'actuel registre des activités de traitement ;
2. d'une violation de l'obligation de désigner un délégué à la protection des données en vertu de l'article 37.1.b) et c) du RGPD dans le chef de la deuxième défenderesse.

5. Le 1er septembre 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 1er septembre 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. Elles 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 des défenderesses a été fixée au 13 octobre 2022, celle pour les conclusions en réplique du plaignant au 3 novembre 2022 et enfin celle pour les conclusions en réplique des défenderesses au 24 novembre 2022.

En ce qui concerne les constatations dépassant l'objet de la plainte, la date limite pour la réception des conclusions en réponse de la deuxième défenderesse a été fixée au 13 octobre 2022.

7. Le 9 septembre 2022, la deuxième défenderesse demande une copie du dossier (art. 95, § 2, 3° de la LCA), qui lui a été transmise le 13 septembre 2022.

8. Le 25 septembre 2022, le plaignant demande une copie du dossier (art. 95, § 25, 3° de la LCA), qui lui a été transmise le 5 octobre 2022.

9. Le 25 septembre 2022, le plaignant accepte de recevoir toutes les communications relatives à l'affaire par voie électronique et manifeste son intention de recourir à la possibilité d'être entendu, ce conformément à l'article 98 de la LCA.

10. Le 28 septembre 2022, la première défenderesse accepte de recevoir toutes communications relatives à l'affaire par voie électronique et demande une copie du dossier (art. 95, § 2, 3° de la LCA), laquelle lui est envoyée le 5 octobre 2022 , et elle indique qu'elle souhaite utiliser la possibilité d'être entendue, conformément à l'article 98 de la LCA.

11. Le 13 octobre 2022, la Chambre Contentieuse reçoit les conclusions en réponse de la première défenderesse concernant les constatations relatives à l'objet de la plainte. Tout d'abord, la première défenderesse décrit la relation de travail tendue avec le plaignant. Les constatations du Service d'Inspection concernant la licéité du traitement, le principe de transparence, le principe de limitation des finalités et le principe de minimisation des données ne sont pas contestées par la première défenderesse. Elle affirme avoir entre-temps mis fin à ces violations. La première défenderesse conteste toutefois les constatations relatives au droit d'accès du plaignant et affirme y avoir donné suite conformément au RGPD. La première défenderesse conteste également la constatation selon laquelle elle n'a pas pris suffisamment de mesures de sécurité. Elle a fait appel à un expert en la matière et a reçu une documentation suffisante pour s'assurer du sérieux des mesures prises par le fournisseur (la deuxième défenderesse).

12. Le 13 octobre 2022, la Chambre Contentieuse reçoit les conclusions en réponse de la deuxième défenderesse concernant les constatations relatives à l'objet de la plainte. La deuxième défenderesse affirme être capable de partager les connaissances exactes sur le système. Elle soutient aussi avoir transmis les informations pertinentes à temps à la première défenderesse. Par ailleurs, la deuxième défenderesse fait valoir qu'elle ne traite pas de données à caractère personnel, et donc pas non plus de données biométriques à caractère personnel, vu que les personnes concernées ne sont pas identifiables pour elle, puisqu'elle ne dispose que de fichiers cryptés. Ces conclusions comportent également la réaction de la deuxième défenderesse concernant les constatations effectuées par le Service d'Inspection en dehors du cadre de la plainte. La deuxième défenderesse affirme qu'elle n'était tenue de désigner un délégué à la protection des données ni en vertu de l'article 37.1.b), ni en vertu de l'article 37.1.c) du RGPD. Entre-temps, la deuxième défenderesse a spontanément désigné un délégué à la protection des données.

13. Le 3 novembre 2022, la Chambre Contentieuse reçoit les conclusions en réplique de la part du plaignant. Tout d'abord, le plaignant fait valoir que la description par la première défenderesse de l'état de la relation de travail entre les deux parties n'est pas pertinente dans le cadre de la présente procédure. En ce qui concerne les constatations du Service d'Inspection à propos de l'objet de la plainte, il en demande confirmation à la Chambre Contentieuse.

14. Le 24 novembre 2022, la Chambre Contentieuse reçoit les conclusions en duplique de la première défenderesse en ce qui concerne les constatations relatives à l'objet de la plainte, dans lesquelles elle réitère ses arguments des conclusions en réponse.

15. Le 24 novembre 2022, la Chambre Contentieuse reçoit les conclusions en duplique de la deuxième défenderesse concernant les constatations relatives à l'objet de la plainte. La deuxième défenderesse se réfère à ses conclusions en réponse et demande en outre à la Chambre Contentieuse de tenir compte des motivations réelles des parties.

16. Le 2 décembre 2022, les parties sont informées du fait que l'audition aura lieu le 17 février 2023.

17. Le 2 décembre 2022, le plaignant notifie qu'il ne souhaite plus être entendu.

18. Le 17 février 2023, les parties présentes sont entendues par la Chambre Contentieuse.

19. Le 22 février 2023, le procès-verbal de l'audition est soumis aux parties ayant comparu.

20. Le 28 février 2023, la Chambre Contentieuse reçoit de la deuxième défenderesse quelques remarques relatives au procès-verbal qu'elle décide de reprendre dans sa délibération.

21. Le 4 juin 2024, la Chambre Contentieuse fait connaître à la première défenderesse son intention de procéder à l'imposition d'une amende administrative ainsi que le montant de celle-ci, afin de lui donner l'occasion de se défendre avant que la sanction soit effectivement infligée.

22. Le 26 août 2024, la Chambre Contentieuse reçoit la réaction de la première défenderesse concernant l'intention d'infliger une amende administrative, ainsi que le montant de celle-ci.

II. Motivation

II.1. Licéité du traitement (art. 5.1, a), 6.1 et 9.2 du RGPD) vis-à-vis de la première défenderesse

23. La question se pose de savoir si le traitement des données à caractère personnel dans le cadre de l'enregistrement du temps par la première défenderesse constitue un traitement licite.

24. Le principe de base de l'article 5.1.a) du RGPD est que les données à caractère personnel ne peuvent être traitées que de manière licite.

II.1.1.1. Catégories (particulières) de données à caractère personnel

25. En vertu de l'article 4.1) du RGPD, les données à caractère personnel désignent "toute information se rapportant à une personne physique identifiée ou identifiable (la "personne concernée")". Est réputée identifiable une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un ou plusieurs éléments spécifiques, propres à son identité physique ou physiologique.

26. Au sens de l'article 4.14) du RGPD, les données biométriques sont les données à caractère personnel résultant d'un traitement technique spécifique, relatives aux caractéristiques physiques, physiologiques ou comportementales d'une personne physique, qui permettent ou confirment son identification unique, telles que des images faciales ou des données dactyloscopiques.

27. L'article 9.1 du RGPD définit les données à caractère personnel particulières en ces termes : "*[...] données à caractère personnel révélant l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle [...].*"

    Les parties ne contestent pas que la première défenderesse intervient en tant que responsable du traitement au sens de l'article 4.7) du RGPD en ce qui concerne l'enregistrement du temps de ses travailleurs sur la base de leurs données biométriques.

28. Compte tenu de ce qui précède, la Chambre Contentieuse constate que l'empreinte digitale constitue une donnée biométrique au sens de l'article 4.14) du RGPD. Vu que celle-ci est utilisée par la première défenderesse afin d'identifier la personne concernée dans le cadre de l'enregistrement du temps, elle constitue également une donnée à caractère personnel particulière au sens de l'article 9.1 du RGPD dans le chef de la première défenderesse.

II.1.1.2. Interdiction de traitement des données biométriques

29. La Chambre Contentieuse examinera ci-après si la première défenderesse a traité de manière licite la catégorie particulière de données à caractère personnel dans le cadre de l'enregistrement du temps de ses travailleurs.

30. Les données à caractère personnel qui sont particulièrement sensibles méritent une protection spécifique car leur traitement peut engendrer des risques élevées pour les libertés et droits fondamentaux. Le traitement de catégories spécifiques de données à

caractère personnel est dès lors interdit en vertu de l'article 9.1 du RGPD, à moins qu'une exception légale s'applique.[1]

31. S'il y a un traitement de catégories particulières de données à caractère personnel conformément à l'article 9.1 du RGPD, le responsable du traitement doit désigner une base juridique conformément à l'article 6 du RGPD ainsi qu'un motif d'exception de l'article 9.2 du RGPD pour qu'il soit question d'un traitement licite. Ce cumul d'un fondement des articles 6.1 et 9.2 du RGPD a récemment été confirmé dans l'arrêt Meta (C-252/21) de la Cour de justice[2] dans lequel la Cour estime expressément que le traitement de données à caractère personnel sensibles n'est permis que si un tel traitement peut être qualifié de licite en vertu de l'article 6.1 du RGPD. L'avis 2/2019 du Comité européen de la protection des données (European Data Protection Board ; ci-après : EDPB)[3] et l'avis 06/2014 du Groupe de travail Article 29 sur la protection des données[4] renvoient également logiquement à l'application tant de l'article 6 du RGPD que de l'article 9 du RGPD dans le cas d'un traitement d'une catégorie particulière de données à caractère personnel. Le considérant 51 du RGPD indique enfin clairement que l'article 6 du RGPD doit toujours être appliqué.

32. Il appartient au responsable du traitement de déterminer quelle est la base légale adéquate au regard de la finalité du traitement.[5] Étant donné que des conséquences différentes découlent de bases légales différentes, notamment en termes de droits pour les personnes concernées, le responsable du traitement n'est pas autorisé à se fonder sur l'une ou l'autre base légale au gré des circonstances. Une fois qu'une base légale déterminée a été choisie, le but n'est pas de passer de l'une à l'autre ou que, lorsque la base légale choisie cesse de s'appliquer, l'on se rabatte sur une autre base légale pour la même activité de traitement, pour les mêmes finalités.[6] L'article 5.1.b) du RGPD exige en effet que les données à caractère personnel "*soient collectées pour des finalités déterminées, explicites et légitimes et ne soient pas traitées ultérieurement d'une manière incompatible avec ces finalités ; [...] ("limitation des finalités*")". Lorsqu'un même traitement poursuit plusieurs finalités, chaque finalité doit être fondée sur une base légale.[7]

33. La question se pose dès lors de savoir quelle base juridique issue des articles 6.1 et 9.2 du RGPD la première défenderesse invoque pour le traitement litigieux d'une catégorie particulière de données à caractère personnel. Après avoir enquêté, le Service d'Inspection

---

[1] Voir le considérant 51 du RGPD.

[2] CJUE, Arrêt du 4 juillet 2023, Meta, C-252/21, ECLI:EU:C:2023:537, para. 90.

[3] Avis 3/2019 (EDPB) concernant les questions et réponses sur l'interaction entre le règlement relatif aux essais cliniques (REC) et le règlement général sur la protection des données (RGPD) (article 70, paragraphe 1, point b)) du 23 janvier 2019.

[4] Avis 06/2014 (WP 29) sur la notion d'intérêt légitime poursuivi par le responsable du traitement des données au sens de l'article 7 de la directive 95/46/CE.

[5] Voir également la décision 74/2023, para. 74, de la Chambre Contentieuse.

[6] Voir par exemple les décisions 38/2021, 54/2023 et 77/2023 de la Chambre Contentieuse.

[7] Voir également la décision 77/2023, para. 77, de la Chambre Contentieuse.

aboutit à la constatation que la documentation fournie ne permet pas d'établir de manière univoque la base juridique précisément invoquée par la première défenderesse pour le traitement litigieux. D'une part, la première défenderesse invoque en effet différentes bases juridiques dans différents documents et d'autre part, elle n'invoque pas une seule mais plusieurs bases juridiques en même temps. En tout cas, le Service d'Inspection constate qu'aucune des bases juridiques invoquées ne peut constituer une base juridique valable pour le traitement litigieux.

34. La première défenderesse ne conteste pas les constatations du Service d'Inspection. Dans ses conclusions, la première défenderesse déclare que lors de la journée d'accueil des nouveaux membres du personnel, le responsable des ressources humaines distribue la brochure d'accueil et que le travailleur donne alors son consentement à l'enregistrement du temps sur la base de ses empreintes digitales. La première défenderesse admet que cette pratique est contraire à la recommandation du Centre de Connaissances de l'APD sur le traitement de données biométriques du 1er décembre 2021, selon laquelle, vu la subordination dans le contexte du travail, il est improbable que la personne concernée puisse refuser son consentement au traitement de données sans crainte de conséquences négatives découlant de ce refus. À titre de circonstance atténuante, la première défenderesse fait valoir que lors de l'introduction du nouveau règlement de travail, aucun travailleur n'a commenté les ajouts concernant le système biométrique. Il était possible de communiquer des remarques de façon anonyme. Aucune délégation syndicale n'en a formulé. En outre, les travailleurs eux-mêmes ont indiqué qu'ils préféraient le système biométrique au système de badges d'accès.

35. En ce qui concerne la licéité du traitement, la Chambre Contentieuse constate que dans ses conclusions en réponse, la première défenderesse ne mentionne pas explicitement sur quelle base juridique de l'article 6.1 *j°* l'article 9.2 du RGPD elle se fonde pour le traitement litigieux. La Chambre Contentieuse relève également qu'au cours de l'enquête, différentes bases juridiques ont été avancées pour le traitement litigieux des données à caractère personnel. Sur la base des conclusions et de l'audition, la Chambre Contentieuse constate que la première défenderesse invoque finalement le consentement comme base juridique. La Chambre Contentieuse vérifie ci-après si la première défenderesse peut légitimement invoquer l'exception du consentement au sens de l'article 9.2.a) du RGPD.

36. L'article 4.11) du RGPD définit le consentement comme toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement.

37. Pour que le consentement soit éclairé, la personne concernée doit être informée entre autres de l'identité du responsable du traitement, de la finalité du traitement, des (types de) données traitées et de l'existence du droit de retirer son consentement.[8]

38. Une personne concernée doit en outre pouvoir donner son consentement librement. Dans les Lignes directrices de l'EDPB sur le consentement au sens du RGPD, la remarque suivante est formulée :

"*Un déséquilibre des rapports de force peut également avoir lieu dans le cadre des relations de travail. Au vu de la dépendance résultant de la relation employeur/employé, il est peu probable que la personne concernée soit en mesure de refuser de donner son consentement à son employeur concernant le traitement de ses données sans craindre ou encourir des conséquences négatives suite à ce refus. Il est ainsi peu probable qu'un employé soit en mesure de répondre librement à une demande de consentement de la part de son employeur visant à activer des systèmes de surveillance, tels que des caméras de surveillance, sur le lieu de travail, ou à remplir des formulaires d'évaluation, sans se sentir obligé de consentir. Aussi l'EDPB considère-t-il problématique que les employeurs traitent les données à caractère personnel de leurs employés actuels ou potentiels en se fondant sur leur consentement, dès lors qu'il est peu probable que celui-ci soit donné librement. Pour la majorité de ces traitements de données au travail, la base juridique ne peut et ne devrait pas être le consentement des employés (article 6, paragraphe 1, point a)) en raison de la nature de la relation employeur/employé. Cela ne signifie toutefois pas que les employeurs ne peuvent jamais avoir recours au consentement en tant que base juridique pour le traitement de données. Il peut exister des situations où l'employeur est en mesure de démontrer que le consentement est de facto donné librement. Vu le déséquilibre des rapports de force entre un employeur et les membres de son personnel, les employés ne peuvent donner librement leur consentement que dans des situations exceptionnelles, lorsqu'absolument aucune conséquence négative ne résultera de leur refus de donner leur consentement [...] Les déséquilibres de rapports de force ne se limitent pas aux autorités publiques et aux employeurs, ils peuvent également avoir lieu dans d'autres situations. Comme souligné par le G29 dans plusieurs avis, le consentement ne peut être valable que si la personne concernée est véritablement en mesure d'exercer un choix et s'il n'y a pas de risque de tromperie, d'intimidation, de coercition ou de conséquences négatives importantes (par ex. coûts supplémentaires importants) si elle ne donne pas son consentement. Le consentement ne sera pas libre lorsque tout élément de contrainte, de pression ou d'incapacité d'exercer un véritable choix sera présent*".

[8] Voir le considérant 42 du RGPD, les Lignes directrices sur le consentement au sens du règlement 2016/679 du 28 novembre 2017, p. 15 et l'article 7, § 3 du RGPD.

39. Au vu de ces éléments, la Chambre Contentieuse souligne que dans une relation de travail, le traitement ne peut être fondé sur le consentement que dans des circonstances exceptionnelles. Elle examine dans quelle mesure une telle circonstance se présente en l'espèce.

40. En vertu de l'article 7.1 du RGPD, le responsable du traitement doit être en mesure de démontrer que la personne concernée a donné son consentement au traitement de données à caractère personnel la concernant.

41. Les conditions de l'article 7 du RGPD s'appliquent également à la notion de consentement visée à l'article 9.2 du RGPD.[9] Pour répondre à la condition de l'article 9.2.a) du RGPD pour une exception à l'interdiction de traitement de données biométriques de l'article 9.1 du RGPD - en plus des conditions définies à l'article 7 RGPD pour le consentement - la personne concernée doit donner son consentement explicite. En d'autres termes, déduire le consentement du fait qu'une personne n'agit ou ne proteste pas n'est pas autorisé.

42. Dans sa réponse du 5 août 2022, la première défenderesse a confirmé au Service d'Inspection que les précédentes versions du règlement de travail datant d'avant la version de juin 2022 ne comportaient aucune disposition relative à un système biométrique d'enregistrement du temps. Il n'est dès lors pas question d'un consentement éclairé.

43. La première défenderesse transmet à la Chambre Contentieuse la brochure d'accueil qui était remise aux nouveaux travailleurs lors de leur entrée en service initiale ainsi que le règlement de travail. Ces documents servent à informer le travailleur à propos du système d'enregistrement du temps. Ces documents ont été signés, mais pour réception et pas pour accord. Bien que ces documents donnent quelques informations - succinctes - aux travailleurs à propos du système d'enregistrement du temps, on ne peut pas conclure sur cette base qu'il s'agisse d'un consentement univoque.

44. En outre, la première défenderesse n'a pas démontré qu'il était question d'un consentement donné librement. La brochure d'accueil mentionne ce qui suit "*[votre] salaire est basé sur vos pointages, veillez donc à ne pas l'oublier ". [NdT : les passages extraits du dossier sont des traductions libres effectuées par le Service Traduction de l'Autorité de protection des données, en l'absence de traduction officielle]. Par ailleurs, l'article 32 du règlement de travail indique que le non respect des règles relatives au pointage peut engendrer des sanctions. Sur la base du rapport d'inspection, la Chambre Contentieuse constate que l'enregistrement du temps par empreintes digitales est le seul moyen d'enregistrement du temps en vigueur. Cela signifie que si une personne concernée refusait de donner son consentement à l'enregistrement du temps par empreintes digitales, elle s'exposerait aux sanctions prévues par le règlement de travail, étant donné qu'aucune autre méthode n'est*

[9] Lignes directrices 2016/679 de l'EDPB sur le consentement au sens du règlement 2016/679 du 28 novembre 2017, p. 23.

prévue pour l'enregistrement du temps. Au contraire, le règlement de travail stipule même que tous les membres du personnel sont obligés d'enregistrer leur temps de travail par le biais de Z, et qu'il n'existe pas d'autre système d'enregistrement du temps de travail, de sorte qu'il n'y a pas de liberté de choix pour les travailleurs. Dès lors, des conséquences négatives sont associées au refus du travailleur de donner son accord. La Chambre Contentieuse relève également que le plaignant était initialement employé en tant que travailleur intérimaire, ce qui le place dans une position encore plus défavorable pour formuler des remarques concernant le système d'enregistrement du temps.

45. La première défenderesse estime que les travailleurs ont donné leur consentement pour l'utilisation de leurs empreintes digitales et que personne ne s'y est jamais non plus opposé. La première défenderesse déclare que le système de badges était perçu comme peu pratique par les travailleurs et qu'elle n'avait que de bonnes intentions. En outre, la première défenderesse fait valoir que les travailleurs pouvaient également indiquer leur souhait d'une autre méthode d'enregistrement du temps. La première défenderesse estime donc que les travailleurs ont pu donner librement leur consentement.

46. La Chambre Contentieuse ne suit pas ce raisonnement. Compte tenu de la dépendance qui résulte de la relation entre l'employeur et le travailleur, il est peu probable que le travailleur puisse donner librement son consentement. La Chambre Contentieuse se réfère dans ce contexte aux lignes directrices de l'EDP sur le consentement[10], selon lesquelles il peut être question d'un rapport de forces déséquilibré dans un contexte de travail. Étant donné qu'en l'espèce, il s'agit d'une relation employeur/travailleur, il est improbable que la personne concernée, en tant que travailleur, puisse refuser de donner son consentement sans crainte ou sans risque réel de conséquences dommageables. La Chambre Contentieuse observe également que ni la brochure d'accueil, ni le règlement de travail à l'époque où le plaignant était employé, ne mentionnaient que d'autres méthodes d'enregistrement du temps pouvaient être demandées. Cependant, lors de l'audition, la première défenderesse a produit des documents montrant que le système d'enregistrement du temps litigieux a été abandonné à la suite des conclusions du Service d'Inspection.

47. Sur la base des faits suivants, la Chambre Contentieuse conclut que la première défenderesse n'a pas démontré que ses travailleurs ont donné leur consentement explicite au traitement de leurs données biométriques. Le consentement spécifique, éclairé et univoque n'a donc pas été établi.

48. La Chambre Contentieuse conclut donc que dans la présente affaire, la première défenderesse a violé l'interdiction de principe de traiter des catégories particulières de données à caractère personnel, vu qu'elle ne peut pas invoquer l'article 6.1.a) *j°* l'article 9.2.a)

[10] https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_fr.pdf.

du RGPD pour le traitement litigieux de catégories particulières de données à caractère personnel, à savoir l'enregistrement du temps sur la base de données biométriques. Il est par conséquent question d'une violation de l'article 9.1 ***j°*** **l'article 6.1.a) et l'article 9.2.a) du RGPD** . Le fait qu'il ait été mis fin aux traitements litigieux suite aux constatations du Service d'Inspection n'empêche pas la constatation de la violation historique.

II.2. Principe de limitation des finalités (article 5.1.b) du RGPD) vis-à-vis de la première défenderesse

49. Pour autant que cela soit nécessaire, la Chambre Contentieuse rappelle que les données à caractère personnel ne peuvent être collectées et traitées que pour des finalités déterminées, explicites et légitimes. Lorsque les données sont utilisées ultérieurement pour une autre finalité, cette nouvelle finalité doit être compatible avec la finalité initiale de la collecte. Le principe de limitation des finalités comporte donc deux éléments :

   a. les données à caractère personnel doivent être traitées pour des finalités déterminées, explicites et légitimes ; et

   b. lorsque des données à caractère personnel sont collectées, elles ne peuvent pas être traitées ultérieurement d'une manière incompatible avec ces finalités.

   Ainsi, le principe de limitation des finalités garantit que des limites sont fixées à l'utilisation des données à caractère personnel, en tenant compte des prévisions raisonnables des personnes concernées et du fait qu'une utilisation ultérieure pour des finalités autres que celles pour lesquelles les données ont été initialement collectées peut également s'avérer utile.

50. Pendant l'enquête d'inspection, la première défenderesse s'est référée à quatre finalités :

   - l'enregistrement du temps de travail permettant l'établissement des fiches de salaires ;
   - la prévention de la fraude lors de l'enregistrement du temps ;
   - des raisons de sécurité, notamment afin de savoir en tout temps combien de personnes sont présentes sur le site de production en cas d'incendie ou de contrôle du changement d'équipes successives ; et
   - le contrôle de l'accès au bâtiment de l'employeur.

51. Le Service d'Inspection observe que la quatrième finalité (contrôle de l'accès au bâtiment) ne figure dans aucun autre document et qu'il ressort de la lettre de la première défenderesse que le traitement pour cette finalité n'avait pas encore été réalisé. Il s'agit donc d'un traitement ultérieur potentiel dont la finalité au sens de l'article 5.1.b) et de l'article 6.4 du RGPD ne peut pas être incompatible avec les finalités initiales. Le Service d'Inspection conclut que le traitement pour le contrôle de l'accès ne sera possible que dans des cas très limités, étant donné qu'il s'agit de données biométriques, et souligne que la collecte initiale

était déjà illicite. Le Service d'Inspection se réfère au règlement de travail (version juin 2022) qui mentionne à deux endroits les trois mêmes finalités que dans la réponse de la première défenderesse : l'enregistrement du temps (y compris la gestion des salaires), la lutte contre la fraude et la sécurité. Le registre des activités de traitement ne mentionne toutefois qu'une seule finalité, à savoir l'enregistrement du temps. Dans la brochure d'accueil, le Service d'Inspection retrouve deux finalités, à savoir l'enregistrement du temps et les raisons de sécurité. Le Service d'Inspection objecte que la finalité de lutte contre la fraude n'apparaît pas dans la brochure d'accueil. C'est important pour le Service d'Inspection car il s'agit du seul document dont la première défenderesse peut démontrer qu'il a été porté à la connaissance du plaignant avant le traitement. Le Service d'Inspection constate dès lors que la condition de collecte pour "des finalités déterminées, explicites et légitimes" n'est pas remplie.

52. Enfin, le Service d'Inspection conclut qu'aucune des finalités ne remplit la condition de légitimité énoncée à l'article 5.1.b) du RGPD. Étant donné que le traitement initial était illicite, toute finalité pour laquelle les données sont collectées est illicite. Par conséquent, le rapport d'inspection indique que dans tous les cas, les finalités citées par la première défenderesse ne sont pas légitimes et que dans certains cas, elles ne sont en outre pas non plus déterminées ni explicites.

53. La première défenderesse fait valoir qu'elle a tenu compte de cette conclusion et qu'elle a l'intention de s'y conformer. Elle a donc immédiatement suspendu tous les projets futurs liés à la sécurisation biométrique du site de son entreprise.

54. La Chambre Contentieuse vérifie ci-après si le principe de limitation des finalités est respecté.

Une finalité déterminée

55. Comme déjà indiqué, une finalité doit être déterminée, ce qui signifie que la finalité de traitement doit être déterminée avant l'obtention des données. Conformément à l'article 13.1 du RGPD, lorsque des données à caractère personnel sont collectées auprès de la personne concernée, le responsable du traitement lui communique la finalité du traitement au moment de l'obtention des données.[11] Par conséquent, seules les deux finalités "enregistrement du temps" et "sécurité du site de l'entreprise" répondent à cette condition, vu qu'elles ont été communiquées au plaignant dans la brochure d'accueil.

Une finalité déterminée et explicite

56. L'explication des finalités peut se faire de différentes manières, par exemple en décrivant les finalités dans une notification aux personnes concernées.[12] La Chambre Contentieuse

[11] https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf, p. 17.

[12] https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf, p. 18.

déclare que la communication des finalités dans la brochure d'accueil peut répondre à cette condition. En outre, la Chambre Contentieuse affirme que le citoyen moyen peut comprendre ce que recouvrent les finalités "enregistrement du temps" et "sécurité du site de l'entreprise".

Une finalité légitime

57. Les données à caractère personnel doivent être obtenues ou collectées pour des finalités légitimes. Pour que les finalités soient légitimes, le traitement doit - à toutes ses étapes et à tout moment - être fondé sur au moins une des bases juridiques citées à l'article 6 du RGPD.[13] Étant donné qu'il a déjà été établi au point II.1 que le traitement n'est pas légitime, il n'est pas non plus question de finalité légitime.

58. Compte tenu de ce qui précède, la Chambre Contentieuse estime **qu'il y a violation de l'article 5.1.b) du RGPD**.

II.3. Principe de minimisation des données (article 5.1.c) du RGPD) vis-à-vis de la première défenderesse

59. Selon le principe de minimisation des données tel que défini à l'article 5.1.c) du RGPD, les données à caractère personnel traitées doivent être adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées. Il en résulte que les données à caractère personnel ne peuvent être traitées que si la finalité du traitement ne peut être raisonnablement atteinte par d'autres moyens. Le traitement doit être proportionnel à la finalité visée.

60. Le Service d'Inspection constate que la première défenderesse ne peut produire aucun document interne ou preuve de délibération ou de processus décisionnel démontrant la mise en œuvre d'un test de proportionnalité. Le Service d'Inspection conclut donc que la première défenderesse n'a pas examiné si la finalité poursuivie n'aurait pas pu être raisonnablement atteinte par d'autres moyens, tels que l'authentification multifactorielle.

61. En ce qui concerne la finalité de "lutte contre la fraude", le Service d'Inspection constate que le système d'enregistrement du temps n'est pas proportionné au cas de fraude qui a donné lieu à l'introduction du système litigieux. Cet incident concernait un travailleur qui avait quitté le travail plus tôt et avait indûment signé le registre de présence papier pour la fin de la journée. Le Service d'Inspection estime qu'un système de contrôle moins intrusif aurait également suffi à détecter et à prévenir de telles fraudes.

62. En ce qui concerne la finalité "sécurité du personnel", à savoir l'assurance que les machines soient systématiquement contrôlées par un travailleur, le Service d'Inspection ne voit pas de lien clair entre cette finalité et le moyen (l'enregistrement des temps litigieux), vu que la

[13] https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf, p. 19

présence d'un travailleur sur le site de l'entreprise n'équivaut pas au contrôle systématique d'une machine particulière, d'autant plus que le pointage de sortie pour les pauses n'est pas requis, selon la brochure d'accueil. Dans le sens où la sécurité incendie doit également être incluse dans la finalité "sécurité du personnel", le Service d'Inspection comprend par contre l'importance d'un registre des présences correct. Le Service d'Inspection souligne toutefois que ce qui importe le plus lors d'une évacuation est de savoir combien de personnes sont présentes dans le bâtiment et à titre secondaire, leur identité.

63. Dans ses conclusions, la première défenderesse s'engage à mettre fin immédiatement au système d'enregistrement du temps sur la base de données biométriques. La première défenderesse explique que ses clients sont très exigeants en matière de sécurité, ce qui fait qu'ils réclament qu'elle obtienne toute une série de certifications auxquelles s'appliquent de nombreuses conditions de sécurité. À cet égard, elle transmet deux documents. Elle fait valoir que l'environnement dans lequel elle doit opérer est très restrictif et que cela l'a amenée à travailler avec le système litigieux de l'enregistrement du temps.

64. La Chambre Contentieuse rappelle que lors de l'évaluation de la nécessité d'utiliser des données personnelles sensibles, telles que des données biométriques, pour tenir à jour les enregistrements du temps de travail, il convient d'examiner les moyens disponibles qui permettent d'atteindre la même finalité d'une manière moins intrusive pour la vie privée des travailleurs. Il est permis de supposer que les employeurs peuvent disposer de nombreux moyens permettant aux travailleurs d'établir une connexion et une déconnexion à un système de rémunération qui ne soit pas basé sur des données biométriques ou d'autres données à caractère personnel sensibles. Citons par exemple des pointeuses, des cartes de personnel et des codes d'accès. En outre, les moyens susmentionnés peuvent être combinés à un contrôle ponctuel ou à un organisme de contrôle lors de l'accès au lieu de travail. La Chambre Contentieuse comprend que la première défenderesse doive répondre aux exigences élevées de ses clients, mais estime en même temps que le traitement de données à caractère personnel particulières n'est pas nécessaire pour atteindre les finalités de la première défenderesse - à savoir l'enregistrement du temps, la lutte contre la fraude ou la sécurité du personnel - et que ces finalités peuvent être atteintes par d'autres mesures moins contraignantes qui ne nécessitent pas le traitement systématique des données biométriques des travailleurs.

65. La Chambre Contentieuse souligne que l'utilisation de données biométriques pour l'identification unique d'une personne est généralement soumise à des limitations très strictes. Ceci est particulièrement pertinent lorsque d'autres mesures moins strictes sont insuffisantes et peut être pertinent lorsque le traitement est destiné au contrôle de l'accès à certaines zones du lieu de travail en raison de considérations de sécurité particulières, telles que la manipulation de denrées alimentaires ou de substances dangereuses

(article 9.2.g) du RGPD). De telles circonstances en sont en l'occurrence pas présentes. La Chambre Contentieuse conclut donc qu'il est question d'une **violation de l'article 5.1.c) du RGPD**.

II.4. Principe de limitation de la conservation (article 5.1.e) du RGPD) vis-à-vis de la première défenderesse

66. Conformément à l'article 5.1.e) du RGPD, "*les données à caractère personnel doivent être conservées sous une forme permettant l'identification des personnes concernées pendant une période n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées*". Concrètement, cela signifie qu'une fois que la finalité du traitement a été réalisée, ou lorsque la base juridique n'est plus valable (par exemple en raison du retrait du consentement par les personnes concernées ou de la disparition de l'intérêt public important), les données biométriques en question doivent être supprimées. Toutefois, cela n'exclut pas que les données soient conservées plus longtemps en vertu d'une obligation légale ou lorsque ces données sont nécessaires dans le cadre d'une procédure judiciaire.

67. Le Centre de Connaissances de l'APD souligne que les données biométriques brutes collectées dans le cadre de la première phase de collecte d'un système biométrique (phase d'enregistrement) doivent en principe immédiatement être supprimées dès que le gabarit biométrique a été créé. En outre, les données collectées lors de la deuxième phase de collecte ne peuvent pas être conservées plus longtemps que le temps nécessaire pour comparer les données collectées avec les informations de référence.[14]

68. En ce qui concerne le principe de limitation de la conservation, le Service d'Inspection ne reçoit aucune référence au délai de conservation de la première défenderesse. Le Service d'Inspection déduit de l'annexe 10 du règlement de travail (version de juin 2022) et du registre des activités de traitement que les données sont conservées pendant toute la durée de la relation de travail. Ces documents n'établissent toutefois aucune distinction entre les données biométriques brutes et les gabarits biométriques qui en découlent. Sur la base de son enquête, le Service d'Inspection conclut que les délais de conservation des données biométriques brutes semblent être conformes aux principes énoncés par le Centre de connaissances de l'APD. Le Service d'Inspection déclare qu'une enquête approfondie n'est pas proportionnée puisque le traitement litigieux s'est déjà avéré illicite sur plusieurs points.

69. La Chambre Contentieuse relève que le Service d'Inspection n'a pas constaté de violation à cet égard et ne voit aucune raison d'adopter un point de vue différent. La Chambre Contentieuse estime donc qu'il n'y a **aucune violation de l'article 5.1.e) du RGPD**.

---

[14] Recommandation 01/2021 relative au traitement de données biométriques, p. 35, consultable via le lien suivant : https://www.autoriteprotectiondonnees.be/publications/recommandation-01-2021-du-1-decembre-2021.pdf.

II.5. Obligations d'information (article 5.1.a) *j°* articles 12.1 et 13 du RGPD) vis-à-vis de la première défenderesse

70. Au cours de son enquête, le Service d'Inspection constate que les obligations d'information prévues à l'article 12.1 et à l'article 13 du RGPD, qui exigent que les informations soient fournies aux personnes concernées au moment où les données à caractère personnel sont obtenues, n'auraient pas été respectées.

71. Sur la base des articles 12.1, 13.1 et 13.2 du RGPD, il est nécessaire que la première défenderesse, en tant que responsable du traitement, fournisse aux personnes concernées des informations concises, transparentes et compréhensibles sur les données à caractère personnel qui sont traitées. Les obligations susmentionnées de transparence constituent une concrétisation de l'obligation générale de transparence figurant à l'article 5.1.a) du RGPD. La Chambre Contentieuse examinera si la première défenderesse a respecté ses obligations d'information.

72. La Chambre Contentieuse lit dans le rapport d'inspection que le Service d'Inspection conclut à une violation des articles 12.1 et 13 du RGPD étant donné que la brochure d'accueil, l'unique document contenant des informations à propos du traitement litigieux qui a été remis au plaignant lors de son entrée en service, ne contenait pas toutes les informations requises par le RGPD. L'article 13 du RGPD définit les informations que le responsable du traitement doit fournir à la personne concernée lorsque les données à caractère personnel sont directement collectées auprès de cette personne, et ce au moment de l'obtention de ces données. Les seules informations destinées aux personnes concernées que le Service d'Inspection peut déduire à partir de la brochure d'accueil sont les suivantes : la catégorie de données à caractère personnel traitées, l'une des finalités explicites de l'enregistrement du temps (à savoir l'enregistrement du temps par empreintes digitales) et une finalité implicite (à savoir la sécurité du personnel). Interrogée une seconde fois à ce sujet, la première défenderesse n'a pas apporté d'éléments nouveaux.

73. Selon les constatations du Service d'Inspection, le règlement de travail (version 2020), qui a été fourni au plaignant lors de son entrée en service, fait uniquement référence à l'utilisation d' "appareils d'enregistrement électroniques" pour la mesure et le contrôle du travail et ne contient que la référence suivante au droit à la protection des données :

"La loi du 8 décembre 1992 relative à la protection de la vie privée et/ou le Règlement général sur la protection des données (RGPD ou GDPR) seront respectés lors du traitement des données à caractère personnel".

74. Selon le Service d'Inspection, les informations ci-dessus ne satisfaisaient pas aux obligations d'information en vertu de l'article 12.1 et 12.3 du RGPD. Dans ses conclusions, la première défenderesse avance que dès l'ouverture de l'enquête d'inspection, elle a

immédiatement pris la mesure des obligations auxquelles elle devait se conformer. Elle a dès lors commencé à adapter ses règles de travail et continuera à les corriger.

75. La Chambre Contentieuse examinera si les obligations d'information sont remplies en vertu de l'article 13 du RGPD *j°* l'article 12.1 du RGPD. Après examen des conclusions de la première défenderesse et des pièces y afférentes, la Chambre Contentieuse constate que la première défenderesse a effectivement pris des mesures en ce sens. Cela ressort du fait qu'elle a joint à ses conclusions un règlement de travail modifié en 2022. Au vu du rapport d'inspection, la Chambre Contentieuse constate qu'à l'époque de l'entrée en service du plaignant, la brochure d'accueil était la seule source d'information pour les travailleurs jusqu'à ce que le règlement de travail soit modifié en juin 2022 (ci-après, le "règlement de travail (version 2022)"). La Chambre Contentieuse examinera donc tout d'abord la brochure d'accueil telle qu'elle s'appliquait au moment de l'entrée en service du plaignant et ensuite le règlement de travail (version 2022), notamment en fonction du système d'enregistrement du temps litigieux.

Brochure d'accueil

76. La brochure d'accueil fournit les informations suivantes concernant le traitement litigieux :

"*Nous utilisons un système d'enregistrement du temps par empreintes digitales. Après la séance d'accueil, vous serez enregistré et vous devrez pointer au début et à la fin de votre service. Nous avons un changement d'équipe court, ce qui signifie que vous devez avoir pointé au moins 5 minutes à l'avance. Votre salaire est basé sur ces pointages, assurez-vous de ne pas l'oublier. Lors de votre pause, vous ne devez pas pointer au début ni à la fin, sauf si vous quittez le site, ceci pour des raisons de sécurité*".

77. En ce qui concerne la mention de l'identité du responsable du traitement dans la brochure d'accueil, la Chambre Contentieuse constate que l'identité de la première défenderesse en tant qu'employeur est implicitement avancée comme étant celle du responsable du traitement, bien que la Chambre Contentieuse souligne qu'il est recommandé de le mentionner de façon explicite. La Chambre Contentieuse constate en outre que la brochure d'accueil ne répond pas à d'autres obligations d'information. En ce qui concerne notamment les délais de conservation (article 13.2.e) du RGPD), les finalités et la base juridique (article 13.1.c) du RGPD), la Chambre Contentieuse constate que ceux-ci ne sont pas (suffisamment) repris dans la brochure d'accueil. Étant donné que la première défenderesse invoque - certes illicitement - le consentement sur la base de l'article 6.1.a) et de l'article 9.2.a) du RGPD, il convenait également d'informer les personnes concernées qu'elles avaient le droit de retirer leur consentement (article 13.2.c) du RGPD). Quant à la mention de la possibilité d'introduire une plainte auprès de l'APD (art. 13.2.d) du RGPD), la Chambre Contentieuse constate qu'elle n'est pas non plus mentionnée dans la brochure d'accueil.

78. Compte tenu de ce qui précède, la Chambre Contentieuse conclut que la brochure d'accueil ne satisfait pas aux obligations d'information prescrites par l'article 13 de la LCA et que les informations contenues dans la brochure d'accueil ne sont pas reprises de manière transparente et compréhensible comme le prévoit l'article 12.1 de la LCA.

Règlement de travail (version 2022)

79. La première défenderesse soutient avoir déjà pris des mesures pour respecter ses obligations d'information, en adaptant le règlement de travail. La Chambre Contentieuse constate que le règlement de travail (version 2022) comporte une annexe 10 intitulée "GDPR en privacybeleid voor werknemers" (RGPD et politique de protection de la vie privée pour les travailleurs).

80. Dans le règlement de travail (version 2022), la Chambre Contentieuse constate ce qui suit en ce qui concerne les obligations d'information relatives au traitement des données biométriques.

81. En ce qui concerne les finalités et la base juridique du traitement (article 13.1.c) du RGPD), la Chambre Contentieuse constate que le règlement de travail (version 2022) prévoit que les données biométriques et les informations relatives à l'enregistrement du temps par empreintes digitales sont traitées sur la base de l'article 6.1.f) du RGPD, à savoir "*le traitement est nécessaire à la réalisation de l'intérêt légitime de [la première défenderesse], recouvrant(i) la protection de l'entreprise au moyen d'un enregistrement du temps fiable, (ii) la garantie de la sécurité du personnel, (iii) le contrôle et la facilitation de l'accès aux locaux de l'entreprise*. En ce qui concerne la licéité de la base du traitement et la base juridique applicable, la Chambre Contentieuse renvoie au point II.1. En outre, la Chambre Contentieuse constate que le règlement de travail (version 2022) satisfait aux obligations d'information en vertu de l'article 13 du RGPD. Les informations sont également présentées de manière schématique, ce qui les rend accessibles de manière concise, transparente et compréhensible pour la personne concernée (article 12.1 du RGPD).

82. Sur la base de ce qui précède, la Chambre Contentieuse constate que la première défenderesse a commis une **violation de l'article 12.1 du RGPD *j°* les articles 13.1.c), 13.2.c), d) et e) du RGPD** pour le manque de transparence dans la brochure d'accueil, et de **l'article 12.1 du RGPD *j°* l'article 3.1.c)** du RGPD en ce qui concerne le règlement de travail (version 2022) depuis l'entrée en vigueur du système d'enregistrement du temps litigieux jusqu'à son arrêt en décembre 2022. Le fait que les violations de l'article 13.2.c), d) et e) aient été résolues n'empêche pas la Chambre Contentieuse de constater une violation historique.

II.6. L'article 12.1 et l'article 15 du RGPD (droit d'accès) vis-à-vis de la première défenderesse

Constatations dans le rapport d'inspection

83. Dans le rapport d'inspection, le Service d'Inspection conclut qu'il est question d'une violation de l'article 5.1.a) *j°* l'article 12.1 et l'article 15 du RGPD concernant le droit d'accès. Le Service d'Inspection constate que le plaignant a exercé son droit d'accès à deux reprises par écrit. La première fois par e-mail le 21 février 2022 et la deuxième fois par envoi recommandé le 31 mars 2022. Pendant l'enquête d'inspection, la première défenderesse soutient avoir répondu oralement à la première demande lors d'une réunion avec le délégué syndical le 15 mars 2022. Le Service d'Inspection peut déduire des échanges d'e-mails entre le secrétaire du syndicat et la première défenderesse, avec le plaignant en copie, que les informations demandées faisaient partie de l'ordre du jour de cette réunion et que l'initiative de la réunion est venue du plaignant par l'intermédiaire de son représentant syndical. Étant donné que l'initiative est venue (indirectement) du plaignant, le Service d'Inspection estime possible, en vertu de l'article 12.1 *in fine* du RGPD, que la première défenderesse puisse légalement donner suite à la demande oralement. Compte tenu de la compétence de représentation de la délégation syndicale établie en Belgique par CCT interprofessionnelle[15] et de la communication préalable par l'intermédiaire du secrétaire syndical en question, la première défenderesse était, selon le Service d'Inspection, raisonnablement en droit de supposer que la demande d'accès pouvait être satisfaite oralement par l'intermédiaire du secrétaire syndical. Le Service d'Inspection conclut donc que la première défenderesse rend plausible le fait d'avoir donné suite à la première demande d'accès datée du 21 février 2022 dans le délai prévu à l'article 12.3 du RGPD.

84. Dans la deuxième demande d'accès datée du 31 mars 2022, le plaignant réitère sa demande initiale et sollicite encore une réponse écrite de la première défenderesse. Cette réponse suit par courrier recommandé le 20 avril 2022. Le Service d'Inspection fait valoir que certaines des questions du plaignant concernaient des éléments d'information figurant dans l'article 13 du RGPD et non dans l'article 15 du RGPD. Vu que la première défenderesse ne s'était pas conformée à l'obligation d'information découlant de l'article 13 du RGPD (au moment de l'exercice du droit d'accès), le Service d'Inspection conclut que la première défenderesse devait également répondre à ces questions. D'après le Service d'Inspection, la réponse de la première défenderesse est incomplète sur les points suivants :

- Seules 2 des 3 finalités sont mentionnées. La finalité de lutte contre la fraude n'est pas mentionnée (article 15.1.a) du RGPD).

[15] Voir la CCT n° 5/1. 5.10.2022 Convention collective de travail n° 5 du 24 mai 1971 concernant le statut des délégations syndicales du personnel des entreprises, modifiée et complétée par la convention collective de travail n° 5 bis du 30 juin 1971, n° 5 du 21 décembre 1978 et n° 5 quater du 5 octobre 2011.

- Le plaignant a demandé s'il pouvait refuser de donner son consentement au traitement et a également affirmé qu'il n'avait jamais donné volontairement un tel consentement. Dans sa réponse, la première défenderesse n'aborde pas cette question mais se contente de mentionner le fait que, selon elle, le consentement a été valablement donné et que les données ont entre-temps été supprimées (depuis le départ du plaignant). Si d'après la première défenderesse, le consentement constituait la base légale applicable pour le traitement, elle aurait dû attirer l'attention du plaignant sur le fait que ce consentement pouvait toujours être retiré, conformément à l'article 13.2.c) du RGPD.
- Si d'après la première défenderesse, le consentement ne constituait pas la base légale applicable, elle aurait dû préciser dans sa réponse sur quelle base légale se fondait le traitement, en vertu de l'article 13.1.c) du RGPD.
- En fonction de la base légale communiquée (comme expliqué ci-avant, la première défenderesse invoque simultanément différentes bases légales), elle aurait ensuite dû respectivement communiquer les intérêts légitimes sur lesquels se fondait le traitement (art. 13.1.d) du RGPD) et le fait que le plaignant avait le droit de s'opposer au traitement (art. 15.1.e) du RGPD) ou - si la première défenderesse invoque une obligation légale - qu'un refus ou une opposition n'était pas possible vu que le traitement était nécessaire au respect d'une obligation légale de la première défenderesse.

85. Le Service d'Inspection note que l'obligation dans le chef de la première défenderesse de répondre de manière complète et exacte à la demande d'accès a subsisté malgré le fait qu'entre la demande initiale du plaignant datée du 21 février 2022 et la réponse datée du 20 avril 2022, le traitement a été interrompu (en raison du départ du plaignant). Le Service d'Inspection n'a pas pu déterminer quelles informations supplémentaires ou différentes éventuelles ont été communiquées verbalement par le secrétaire du syndicat lors de la réunion du 15 mars 2022.

Position de la première défenderesse

86. Dans ses conclusions, la première défenderesse reprend la demande d'accès du 21 février 2022. La première défenderesse en déduit les questions suivantes du plaignant :

(i) La politique relative aux personnes ayant accès à la section "admin" de la pointeuse ;

(ii) La possibilité de refuser l'utilisation du système biométrique ;

(iii) La disparition de cet accès administratif et le responsable de la mise hors service ;

(iv) Le délai de conservation et les modalités de conservation ; et

(v) La sécurité des données à caractère personnel.

87. Selon la première défenderesse, les deux premières questions n'étaient plus pertinentes au moment du second courrier daté du 31 mars 2022, le plaignant ayant été licencié le 24 février 2022. Toutefois, la question (i) a fait l'objet de réponses orales et écrites. Concernant la question (ii), la première défenderesse fait valoir qu'il n'a nullement été démontré que le plaignant n'aurait pas eu le droit de choisir un autre système d'enregistrement du temps, étant donné que le plaignant a été licencié le 24 février 2022. Le plaignant est le seul travailleur qui s'est plaint du fait de ne pas avoir consenti à ce que l'on prenne ses empreintes digitales. Par conséquent, on ne peut pas supposer que la première défenderesse aurait refusé une telle alternative si le plaignant était resté sur la liste des salariés. À cet égard, la première défenderesse soulève qu'aucun autre travailleur n'a émis de remarques sur le système biométrique au moment de son introduction dans le nouveau règlement de travail (version 2022).

88. En ce qui concerne la question (iii), la première défenderesse confirme qu'il a été répondu oralement - lors de la réunion du 15 mars 2022 avec le représentant syndical - que le plaignant ne courrait aucun risque. La première défenderesse ne disposait en effet plus des données biométriques du plaignant. Ceci a également été confirmé par écrit.

89. La question (iv) n'était, selon la première défenderesse, plus pertinente puisque les données avaient déjà été supprimées du système au moment de la réponse au droit d'accès. La première défenderesse souligne que le plaignant a été licencié trois jours après avoir exercé son droit d'accès. En même temps et depuis le 3 février 2022, il est représenté par le délégué syndical qui confirme un rendez-vous le 15 mars 2022 pour discuter notamment de ces questions spécifiques. La question (v) n'était également plus pertinente, selon la première défenderesse. Ses données à caractère personnel ayant déjà été supprimées, le plaignant ne courrait plus de risque à cet égard.

90. La première défenderesse conclut dès lors que l'on ne peut pas lui reprocher de ne pas avoir répondu aux demandes du plaignant datées du 21 février 2022 et du 31 mars 2022 dans la mesure où l'exercice de ce droit n'avait plus d'intérêt légitime. En effet, les données à caractère personnel du plaignant ont été supprimées et il le savait ou aurait raisonnablement dû le savoir au vu de la réunion du 15 mars 2022.

Évaluation par la Chambre Contentieuse

91. D'après le rapport d'inspection, la Chambre Contentieuse constate que le plaignant a exercé son droit d'accès pour la première fois le 21 février 2022. Le dossier contient une correspondance par e-mail dont la Chambre Contentieuse peut déduire, d'après les constatations du Service d'Inspection, qu'une concertation a eu lieu le 15 mars 2022, au cours de laquelle une réponse a été apportée aux questions du plaignant. Toutefois, le plaignant lui-même n'était pas présent lors de ces discussions, mais s'est fait représenter par le délégué syndical, ce que déclare également le délégué syndical lui-même. Dans ses

Lignes directrices 01/2022 relatives aux droits des personnes concernées - droit d'accès[16], le Comité européen de la protection des données (ci-après : "EDPB") indique que le droit d'accès est généralement exercé par la personne concernée elle-même, mais qu'il n'est pas exclu qu'un tiers puisse présenter la demande au nom de la personne concernée. Étant donné qu'un tel pouvoir de représentation n'est pas régi dans le RGPD, il convient - comme le fait également remarquer le Service d'Inspection - de se tourner vers les règles nationales applicables, en l'occurrence les CCT belges applicables, comme expliqué par le Service d'Inspection dans le rapport d'inspection. Ces règles permettent au délégué syndical de représenter le plaignant lors de l'exercice du droit d'accès. Au vu des e-mails du 28 février 2022 et du 2 mars 2022 adressés par le délégué syndical à la première défenderesse, cette dernière pouvait légitimement supposer que ce dernier représenterait le plaignant lors de l'entretien du 15 mars 2022. Lors de cet entretien, le système d'enregistrement du temps via des données biométriques devait également être discuté. En effet, l'e-mail du 28 février 2022 du délégué syndical indique que le plaignant souhaite plus de clarté sur ses droits en tant que travailleur et sur le fonctionnement du système biométrique.

92. Toujours dans les Lignes directrices 1/2022 précitées, l'EDPB aborde la manière dont il convient d'octroyer l'accès aux données à caractère personnel. Cela doit principalement se faire au moyen d'une copie des données, mais d'autres modalités, telles que des informations verbales, peuvent suffire si la personne concernée en fait la demande. Étant donné que la proposition d'entretien émanait du délégué syndical, la première défenderesse peut légalement communiquer oralement les informations demandées et donc répondre licitement à la demande d'accès.

93. Au vu de ce qui précède, la première défenderesse pouvait licitement supposer que le délégué syndical, en tant que représentant du plaignant, communiquerait au plaignant les informations fournies par la première défenderesse lors de l'entretien du 15 mars 2022.

94. Compte tenu de ce qui précède et conformément aux conclusions du Service d'Inspection, la Chambre Contentieuse conclut que la première défenderesse a licitement donné suite au droit d'accès du plaignant, selon les modalités sollicitées par le représentant du plaignant.

95. La Chambre Contentieuse attire l'attention sur le fait que l'entretien susmentionné entre la première défenderesse et le représentant du plaignant a eu lieu le 15 mars 2022.

96. Le 31 mars 2022, le plaignant a exercé son droit d'accès une seconde fois. Le plaignant y affirmait que la première défenderesse n'avait pas répondu sur le fond à son e-mail du

[16] EDPB,

Lignes directrices 01/2022 sur les droits des personnes concernées — Droit d'accès 2.0., 17 mars 2023, à consulter via https://www.edpb.europa.eu/system/files/2023-04/edpb_guidelines_202201_data_subject_rights_access_v2_fr.pdf. À l'époque de la demande d'accès du plaignant, la première version s'appliquait, à consulter via https://www.edpb.europa.eu/system/files/2022-01/edpb_guidelines_012022_right-of-access_0.pdf.

21 février 2022. Cette absence de réponse aurait poussé le plaignant à introduire la présente plainte auprès de l'APD.

97. La Chambre Contentieuse rappelle que le droit d'accès n'est pas absolu. L'article 12.5 du RGPD prévoit que lorsque les demandes d'une personne concernée sont manifestement infondées ou excessives, notamment en raison de leur caractère répétitif, le responsable du traitement peut exiger le paiement de frais raisonnables ou refuser de donner suite à ces demandes. Comme le stipule également le considérant 63 du RGPD, la personne concernée peut exercer son droit d'accès facilement et à des intervalles raisonnables. L'EDPB identifie quatre critères permettant à un responsable du traitement de déterminer si l'exercice du droit d'accès est excessif :

(i) La fréquence à laquelle les données à caractère personnel sont modifiées ;

(ii) La nature des données à caractère personnel ;

(iii) La finalité du traitement, entre autres le fait que le traitement a ou non des conséquences négatives pour le plaignant ;

(iv) Si les demandes successives portent sur les mêmes informations demandées ou le même traitement, ou sur des informations ou traitements différents.

98. En appliquant les critères ci-dessus à l'affaire précitée, la Chambre Contentieuse parvient aux conclusions suivantes. En ce qui concerne le premier critère, la Chambre Contentieuse relève que les données biométriques sont propres à la personne concernée et ne sont donc pas modifiées. De même, les heures de pointage enregistrées sur la base des empreintes digitales ne changent plus et ne sont pas non plus complétées, vu le licenciement du plaignant le 24 février 2022. La nature des données à caractère personnel, qui sont des données biométriques, est plutôt sensible, ce qui peut réduire la durée du "délai raisonnable" susmentionné. La finalité du traitement, c'est-à-dire le troisième critère, est la sécurité du personnel, l'enregistrement du temps en vue du calcul des salaires et la prévention de la fraude au pointage, bien que cette finalité ne soit pas toujours mentionnée par la première défenderesse. En soi, ces finalités ne sont pas de nature à avoir un impact négatif sur la personne concernée. En outre, la demande du 31 mars 2022 porte sur les mêmes informations que celles données le 15 mars 2022 suite à l'exercice du droit d'accès par le plaignant en date du 21 février 2022.

99. La Chambre Contentieuse observe que le Service d'Inspection a fait valoir que le licenciement du plaignant le 24 février 2022 n'empêche pas que la première défenderesse doive répondre de manière exhaustive et correcte à la demande d'accès. La Chambre Contentieuse rappelle que le responsable du traitement doit effectivement répondre de manière complète ; toutefois, si la demande du plaignant était limitée à un traitement

spécifique, les informations fournies par le responsable du traitement pourraient également être limitées à ce traitement spécifique.[17] Vu que le plaignant, par l'intermédiaire du délégué syndical en sa qualité de représentant du plaignant, a limité sa demande au système d'enregistrement du temps via des données à caractère personnel biométriques et aux aspects connexes tels que le délai de conservation et la sécurité de ces données à caractère personnel, la Chambre Contentieuse estime que les informations fournies par le responsable du traitement peuvent être limitées à ce traitement spécifique.

100. En ce qui concerne la position de la première défenderesse selon laquelle elle n'avait plus à répondre aux questions 4 et 5 du plaignant parce que les données à caractère personnel avaient déjà été effacées, la Chambre Contentieuse rappelle que le droit d'accès est la "porte d'entrée" qui permet l'exercice des autres droits que le RGPD confère à la personne concernée, tels que le droit de rectification, le droit à l'effacement et le droit à la limitation du traitement[18]. Le raisonnement selon lequel certaines informations ne doivent plus être communiquées pour le passé, par exemple parce que les données ont été effacées, ne peut pas être suivi. Cela empêcherait en effet l'exercice efficace de ces droits.[19] Étant donné que les données à caractère personnel ont été effacées peu avant le licenciement et que le système d'enregistrement du temps par empreintes digitales était encore en place au moment des demandes d'accès, la Chambre Contentieuse estime que la première défenderesse n'aurait pas dû déployer des efforts disproportionnés pour répondre aux questions 4 et 5 de la deuxième demande d'accès. Par ailleurs, la Chambre Contentieuse souligne également que si l'article 15 du RGPD ne prévoit pas que des informations sur les mesures de sécurité doivent être fournies dans le cadre d'une demande d'accès, cela ne signifie pas que, par conséquent, aucune suite ne doit être apportée au droit d'accès. En effet, la première défenderesse pouvait fournir des informations sur les mesures de sécurité au plaignant de manière plus générale.

101. Compte tenu de ce qui précède, la Chambre Contentieuse constate que la première défenderesse a licitement exécuté la demande d'accès du plaignant en ce qui concerne la première demande d'accès datée du 21 février 2022 et les questions 1 à 3 de la deuxième demande d'accès datée du 31 mars 2022. La Chambre Contentieuse constate toutefois que la première défenderesse n'a pas fourni de réponse satisfaisante aux questions 4 et 5 de la

[17] EDPB, Lignes directrices 01/2022 sur les droits des personnes concernées — Droit d'accès, 18 janvier 2022, para. 35. Consultable via le lien suivant : https://www.edpb.europa.eu/system/files/2024-04/edpb_guidelines_202201_data_subject_rights_access_v2_fr.pdf.

[18] Voir l'arrêt le plus récent de la CJUE, 12 janvier 2023, *Österreichische Post AG*-, C-154/21, ECLI:EU:C:2023:3, par. 38, mais aussi CJUE, *17 juillet 2014*, *-YS et al*., C-141/12 -et C-372/12, EU:C:2014:2081, par. 44, et CJUE 20 décembre *2017, -Nowak,* C-434/16, EU:C:2017:994, par. 57, voir également la décision 15/2021 du 9 février 2021, par. 141, et la décision 41/2020 du 29 juillet 2020, par. 47.

[19] CJUE du 9 mai 2009, *Rijkeboer*, C-553/07, ECLI:EU:C:2009:293, para. 54.

deuxième demande d'accès datée du 31 mars 2022, **ce qui entraîne une violation de l'article 12.1 *j°* l'article 15.1.d) du RGPD.**

II.7. L'article 28.1 du RGPD vis-à-vis de la première défenderesse

102. Conformément à l'article 28.1 et au considérant 81 du RGPD, la première défenderesse a, en tant que responsable du traitement, l'obligation d' "*uniquement faire appel à des sous-traitants qui présentent des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées*".

103. Le Service d'Inspection constate que la première défenderesse n'a pas rempli son obligation de diligence requise *(due diligence)* consistant à évaluer l'adéquation des mesures techniques et organisationnelles prises par la deuxième défenderesse. Le Service d'Inspection constate que la première défenderesse a seulement reçu la brochure de vente du système d'enregistrement du temps de la part de la deuxième défenderesse dans la phase préalable à la relation contractuelle. Dans ce document, les informations techniques relatives à la sécurité sont toutefois rares et n'ajoutent rien aux informations succinctes reprises dans le contrat de sous-traitance. D'après le rapport d'inspection, le seul élément qui n'était pas repris dans le contrat de sous-traitance et qui figure par contre dans la brochure est la précision selon laquelle lorsque les données sont envoyées du terminal au serveur, le cryptage est conforme au protocole HTTPS.

104. Suite à la première lettre du Service d'Inspection à la première défenderesse, cette dernière a demandé des informations supplémentaires à la deuxième défenderesse afin de démontrer que le niveau de sécurité appliqué était suffisant. Le Service d'Inspection fait remarquer que cette documentation aurait dû être réclamée préalablement au traitement et pas au moment de l'annonce d'un contrôle du Service d'Inspection. Le Service d'Inspection attire l'attention sur le fait que la première et la deuxième défenderesses confirment qu'un tel échange de documentation n'a pas eu lieu plus tôt. Par conséquent, le Service d'Inspection conclut que le premier responsable ne peut démontrer qu'il a effectivement vérifié les garanties offertes par le sous-traitant en ce qui concerne les mesures techniques et organisationnelles adaptées aux risques associés au traitement litigieux des données à caractère personnel biométriques, ce qui constitue une violation de l'article 28.1 du RGPD.

II.7.1. Position de la première défenderesse

105. La première défenderesse conteste la constatation selon laquelle elle n'a pas pris suffisamment de mesures de sécurité. Elle a fait appel à un expert en la matière et a reçu une documentation suffisante pour s'assurer du sérieux de la deuxième défenderesse en tant que fournisseur. Elle fait valoir que par inadvertance, une annexe au contrat de sous-traitance n'a pas été communiquée. Cette annexe fait partie du contrat de sous-traitance

conclu entre les parties et contient des garanties très spécifiques concernant la sécurité du traitement. Par conséquent, le contenu du contrat de sous-traitance ne se limite pas à une simple description des mesures de sécurité générales de la deuxième défenderesse, mais contient en fait une description détaillée de ce qui est effectivement mis en œuvre. Les catégories de données sont affichées dans l'application sur la base des informations préalablement fournies au Service d'Inspection. La première défenderesse a en effet effectué un choix parmi les différentes possibilités offertes par la deuxième défenderesse. Il n'est donc pas question d'une violation de l'article 28, paragraphe 1 du RGPD.

106. En outre, lors de l'enquête d'inspection, la deuxième défenderesse a produit de la documentation qui se trouve en la possession de la première défenderesse depuis la conclusion du contrat de sous-traitance. Ces documents ont été produits parce qu'ils ont fait l'objet d'un échange entre les parties, ce qui démontrerait que la première défenderesse a bel et bien fait preuve de *due diligence*. La première défenderesse objecte que les preuves du Service d'Inspection ne démontrent pas clairement que les documents relatifs à la sécurité n'ont été produits qu'à la fin de l'enquête d'Inspection et pas préalablement au traitement des données. En outre, la première défenderesse soutient que le Service d'Inspection ne démontre pas que le seul document relatif à la documentation contractuelle est la "brochure de vente". La première défenderesse fait remarquer que le Service d'Inspection n'a pas pris note de sa réponse complète. Dans sa réponse, la première défenderesse avait en effet indiqué que le responsable commercial de la première défenderesse ne travaillait plus pour la société.

II.7.2. Évaluation par la Chambre Contentieuse

107. Le responsable du traitement a l'obligation de faire "uniquement appel à des sous-traitants qui présentent des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière à ce que le traitement réponde aux exigences du RGPD - y compris la sécurité du traitement - et garantisse la protection des droits des personnes concernées.[20] Il incombe donc au responsable du traitement d'évaluer les mesures prises par le sous-traitant et il doit pouvoir démontrer qu'il a sérieusement pris en considération tous les éléments mentionnés dans le RGPD, ce que l'on appelle l'obligation de *due diligence*. Ceci implique généralement un échange de documents tels que, par exemple, la déclaration de confidentialité, les conditions générales et le registre des activités de traitement.

108. L'évaluation ci-dessus doit être effectuée par le responsable du traitement au cas par cas et dépendra fortement du type de traitement confié au sous-traitant, en tenant compte de la

[20] Article 28, paragraphe 1 et considérant 81 du RGPD.

nature, de la portée, du contexte et des finalités du traitement, ainsi que des risques pour les droits et libertés des personnes physiques.

109. Les éléments suivants doivent être pris en considération par le responsable du traitement pour évaluer les garanties : l'expertise du sous-traitant (par exemple, l'expertise technique en ce qui concerne les mesures de sécurité et les violations de données), la fiabilité du sous-traitant et les ressources du sous-traitant.[21] La réputation du sous-traitant sur le marché peut également constituer un facteur pertinent à prendre en considération par le responsable du traitement. En outre, le fait de souscrire à un code de conduite ou à un mécanisme de certification approuvés peut être utilisé pour démontrer l'existence de garanties suffisantes.

110. L'obligation reprise à l'article 28.1 du RGPD de faire uniquement appel à des sous-traitants "présentant des garanties suffisantes" constitue une obligation permanente. Elle ne cesse pas lorsque le responsable du traitement et le sous-traitant concluent un contrat ou un autre acte juridique. Au contraire, le responsable du traitement doit vérifier à des intervalles appropriés les garanties du sous-traitant, entre autres au moyen d'audits et d'inspections si nécessaire.[22]

111. La Chambre Contentieuse constate que le contrat de sous-traitance se compose de trois parties, comme indiqué dans les conclusions de la deuxième défenderesse, à savoir le contrat principal proprement dit avec 2 annexes (Enclosure 1 et Enclosure 2). L'annexe 2 du contrat principal comprenait deux annexes, à savoir le 'Z IT Guide' et un document intitulé "*data processing agreement*". Comme l'a également souligné la deuxième défenderesse, la Chambre Contentieuse observe que le Z IT Guide était absent du dossier d'Inspection, de sorte qu'il n'a pas été pris en compte au cours de l'enquête.

112. La Chambre Contentieuse estime que la description de ces mesures de sécurité permet à la première défenderesse de faire preuve de la *due diligence* nécessaire concernant l'expertise de la deuxième défenderesse en tant que sous-traitant. Tant la première défenderesse que la deuxième défenderesse indiquent que différents échanges ont eu lieu entre les deux parties préalablement à la conclusion du contrat de sous-traitance, mais que les personnes impliquées ne travaillent plus pour les entreprises. Par conséquent, aucune information supplémentaire ne peut être fournie à propos de ces échanges. Pour autant que nécessaire, la Chambre Contentieuse fait remarquer que, dans le cadre du principe de responsabilité, de tels échanges devraient idéalement être documentés afin qu'il y ait une clarté à leur sujet, même après le départ des personnes concernées.

[21] Considérant 81 du RGPD.

[22] Article 28, paragraphe 3, h) du RGPD.

113. Compte tenu de ce qui précède, la Chambre Contentieuse estime que les documents soumis, y compris le contrat de sous-traitance avec ses annexes, montrent que la première défenderesse a pu déployer les efforts nécessaires pour évaluer l'adéquation de la deuxième défenderesse en tant que sous-traitant. Par conséquent, il n'y a **pas de violation de l'article 28.1 du RGPD**..

II.8. L'article 32 du RGPD vis-à-vis de la première défenderesse

II.8.1. Constatations dans le rapport d'inspection

114. Lors de son enquête, le service d'Inspection constate qu'il est question d'une violation de l'article 32 du RGPD dans le chef de la première défenderesse en tant que responsable du traitement.

115. 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*".

116. Dans le prolongement de l'article 5.1.f) du RGPD, l'article 32.1 du RGPD dispose que le responsable du traitement doit mettre en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque. À cet égard, il faut tenir compte de l'état de la technique, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que de la probabilité et de la gravité des risques que présente le traitement pour les droits et libertés des personnes.

117. L'article 32.1 du RGPD dispose également que lors de l'évaluation du niveau de sécurité approprié, il faut tenir compte 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.

118. Le Service d'Inspection affirme que la première défenderesse n'a pas pu démontrer qu'elle disposait de la moindre politique de sécurité de l'information ou de procédures écrites concernant la protection des données à caractère personnel. L'annexe 10 du règlement de travail version 2022 ne figurait pas dans la version du règlement de travail en vigueur au moment du traitement litigieux et a été rédigée après le premier contact avec le Service d'Inspection. De plus, selon le Service d'Inspection, les mesures de sécurité qui y sont reprises ne sont pas suffisamment concrètes pour permettre au Service d'Inspection de se prononcer sur leur pertinence.

119. Le registre des activités de traitement, qui a également été mis en place après le premier contact avec le Service d'Inspection, ne contient pour le traitement litigieux que la description selon laquelle "seul le service RH a accès à ces données. Les dossiers du personnel sont conservés de manière sécurisée sur le serveur et sont conservés physiquement dans une armoire verrouillée dont seul le service RH a la clé. L'enregistrement du temps est traité sur un ordinateur distinct auquel seul le service RH a accès". Dans un deuxième courrier du Service d'Inspection à la première défenderesse, des éclaircissements ont à nouveau été demandés sur les mesures techniques et organisationnelles mises en œuvre dans le cadre de la sécurité de l'information. Un deuxième élément de preuve a été fourni par la première défenderesse, mais le Service d'Inspection a constaté que cet élément de preuve démontrait seulement que le logiciel de la deuxième défenderesse permettait d'affiner le niveau d'accès au sein de la première défenderesse à l'aide de différents rôles. La manière dont l'accès au sein de la première défenderesse a été concrètement mis en oeuvre ne peut être établie par le Service d'Inspection, ce qui ne permet pas de démontrer l'existence d'une politique interne de gestion logique des accès aux données du système d'enregistrement du temps. Le Service d'Inspection ajoute à cela qu'une politique de sécurité de l'information générale fait en tout cas défaut. Selon le Service d'Inspection, il est par conséquent question d'une violation de l'article 32 du RGPD.

II.8.2. Évaluation par la Chambre Contentieuse

120. La première étape pour définir le niveau de sécurité approprié du traitement de données à caractère personnel est de cerner les risques de ce traitement et d'en établir une pondération. Sur cette base, il convient de déterminer quelles mesures sont nécessaires pour prévoir une sécurité suffisante contre ces risques. Il résulte du RGPD que pour la pondération des risques en matière de sécurité des données, il convient de prêter attention aux risques qui peuvent survenir lors du traitement de données à caractère personnel, comme la divulgation non autorisée ou l'accès non autorisé aux données traitées. Lors de l'inventaire et de l'évaluation des risques, ce sont surtout les conséquences d'un traitement illicite de données à caractère personnel que les personnes peuvent subir qui sont pertinentes. Selon que les données ont un caractère plus sensible, ou si le contexte dans lequel celles-ci sont utilisées représente une menace plus importante pour la vie privée, des exigences plus strictes sont posées pour la sécurité des données à caractère personnel.

121. Sur la base du rapport d'inspection, la Chambre Contentieuse constate qu'il n'y avait pas de politique de sécurité de l'information générale disponible concernant le traitement des données biométriques. Après un premier contact avec le Service d'Inspection, la première défenderesse a adapté son registre des activités de traitement et y a inclus les mesures de sécurité.

122. En ce qui concerne les mesures techniques, la Chambre Contentieuse constate que la deuxième défenderesse, en tant que fournisseur du système, prévoit le cryptage nécessaire (certifié ISO). Sur la base du rapport d'inspection, la Chambre Contentieuse constate que plusieurs mesures organisationnelles ont été prises, telles que la limitation des employés ayant accès à ces données à caractère personnel, la limitation de la zone d'accès dans laquelle se trouvaient les données à caractère personnel, la conservation des données à caractère personnel sur un serveur dans une pièce fermée à clé et la conservation des dossiers du personnel papier dans une pièce fermée à clé.

123. En ce qui concerne les constatations relatives à la politique de suivi des mesures de sécurité, la Chambre Contentieuse souligne qu'il convient de faire une distinction entre les mesures de sécurité elles-mêmes et leur documentation dans le cadre du principe de responsabilité. En ce qui concerne les mesures de sécurité proprement dites, la Chambre Contentieuse constate qu'elles répondent aux exigences de l'article 32 du RGPD. Compte tenu de ce qui précède, la Chambre Contentieuse ne constate aucune violation de **l'article 32** du RGPD.

II.9. L'analyse d'impact relative à la protection des données (article 35 du RGPD) vis-à-vis de la première défenderesse

124. Le Service d'Inspection conclut dans son rapport d'inspection qu'il n'est pas clair de savoir si la première défenderesse soutient qu'elle n'était pas tenue d'effectuer une analyse d'impact relative à la protection des données (ci-après : AIPD) parce que le traitement n'était pas susceptible de présenter un risque élevé au sens de l'article 35.1 du RGPD, ou si elle a effectué une AIPD ayant abouti à la conclusion qu'il n'y avait pas de risque résiduel élevé au sens de l'article 36 du RGPD. Dans les deux cas, le Service d'Inspection constate que la première défenderesse n'a pas agi conformément au RGPD.

125. La première défenderesse n'a pas pris position à ce sujet.

126. Conformément à l'article 35.1 du RGPD, le responsable du traitement devra effectuer, avant le traitement, une analyse de l'impact des opérations de traitement envisagées sur la protection des données à caractère personnel lorsque le traitement, en particulier par le recours à de nouvelles technologies, et compte tenu de la nature, de la portée, du contexte et des finalités du traitement, est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques.

127. Comme il ressort du point 6 de la décision n° 01/2019, il faudra toujours réaliser une AIPD lorsque le traitement utilise des données biométriques en vue de l'identification unique des personnes concernées se trouvant dans un lieu public ou dans un lieu privé accessible au public. Toutefois, le Centre de Connaissances de l'APD souligne dans sa recommandation que le traitement de données biométriques pour des finalités autres que celles

expressément reprises dans la décision 01/2019 du Secrétariat général est également soumis, le cas échéant, à l'obligation d'effectuer une AIPD. Qui plus est, vu le risque inhérent élevé pour les droits et libertés des personnes concernées qu'implique le traitement de données biométriques, ne pas réaliser d'AIPD ne sera justifié que dans des cas exceptionnels.

128. Conformément à l'article 35 du RGPD, une AIPD doit être effectuée lorsqu'un traitement de données à caractère personnel est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes concernées. Lors de l'évaluation de la nécessité d'une AIPD, plusieurs facteurs doivent être pris en compte tels que la nature, la portée, le contexte et les finalités du traitement, ainsi que les risques potentiels pour les droits et libertés des personnes concernées.

129. Pour donner une vision plus concrète des opérations de traitement qui nécessitent une AIPD du fait d'un risque inhérent élevé, compte tenu des éléments particuliers de l'article 35.1 et 35.3, points a) à c), de la liste à établir au niveau national en vertu de l'article 35.4, et des considérants 71, 75 et 91, ainsi que des autres références du RGPD aux opérations de traitement "*susceptibles d'engendrer un risque élevé*", le Groupe 29 a élaboré les neuf critères suivants qu'il convient de prendre en compte.[23]

130. La Chambre Contentieuse estime que la plupart de ces critères sont remplis, à savoir :

- Premier critère : évaluation, y compris les activités de profilage et de prédiction, portant notamment sur des "aspects concernant le rendement au travail de la personne concernée". Cette condition est remplie car l'enregistrement du temps de travail d'un travailleur est une caractéristique relative à la performance professionnelle.

- Deuxième critère : prise de décision automatisée avec effet juridique ou effet similaire significatif. Comme déjà expliqué, les travailleurs de la première défenderesse ne disposaient d'aucune alternative démontrée en termes d'enregistrement du temps de travail et aucun salaire ne pouvait être versé si les travailleurs n'enregistraient pas leur temps de travail.

- Quatrième critère (données sensibles ou données à caractère hautement personnel). Il s'agit entre autres des catégories particulières de données à caractère personnel visées à l'article 9 du RGPD, dont les données biométriques utilisées en vue de l'identification.

- Cinquième critère (données traitées à grande échelle). Le RGPD ne précise pas ce qu'il faut entendre par "à grande échelle" mais le Groupe 29 recommande de prendre en compte des facteurs tels que le nombre de personnes concernées, soit en valeur

[23] Groupe de travail Article 29, "*concernant l'analyse d'impact relative à la protection des données (AIPD) et la manière de déterminer si le traitement est 'susceptible d'engendrer un risque élevé'* aux fins du règlement (UE) 2016/679, ratifiées le 4 octobre 2017 (WP 248 rev. 01), p. 9 e.s.

absolue, soit en proportion de la population considérée.[24] Dans le cas présent, l'enregistrement du temps par empreintes digitales concerne tous les travailleurs de la première défenderesse, de sorte qu'il peut s'agir d'un traitement à grande échelle.

- Septième critère : données concernant des personnes vulnérables. Comme indiqué, les travailleurs sont, dans le cas présent, des personnes concernées vulnérables car ils sont dans un rapport de dépendance par rapport à la première défenderesse en tant que leur employeur.

131. Dans la plupart des cas, un responsable du traitement peut partir du principe que si un traitement répond à deux critères, une AIPD doit être réalisée. Comme expliqué ci-dessus, cinq des critères définis sont remplis. La Chambre Contentieuse ajoute que l'utilisation de données biométriques pour l'enregistrement du temps des travailleurs peut engendrer des risques importants pour la vie privée des personnes concernées, tels que le risque élevé d'accès non autorisé, de piratage et d'usurpation d'identité. **Compte tenu de ce qui précède, la Chambre Contentieuse estime que la première défenderesse aurait dû procéder à une AIPD, ce qui entraîne une violation de l'article 35 du RGPD.**

II.10. Transfert vers des pays tiers ou à des organisations internationales (chapitre V du RGPD) vis-à-vis de la première défenderesse

II.10.1. Constatations dans le rapport d'inspection

132. Le Service d'Inspection constate que d'après les documents, les serveurs utilisés sont uniquement situés sur le territoire belge. La première défenderesse indique également dans sa réponse et dans son registre des activités de traitement qu'aucun transfert n'a lieu. D'après la réponse de la deuxième défenderesse, les gabarits ne peuvent pas non plus être extraits par la première défenderesse, ce qui semble exclure le risque d'un éventuel transfert de ces fichiers par la première défenderesse. Par conséquent, le Service d'Inspection conclut qu'il n'existe aucune indication de transferts éventuels de données biométriques vers des pays tiers ou à des organisations internationales.

II.10.2. Évaluation par la Chambre Contentieuse

133. Comme déjà indiqué, le Service d'Inspection ne voit aucune indication de transferts éventuels de données biométriques vers des pays tiers ou à des organisations internationales. La Chambre Contentieuse ne dispose d'aucune indication pour en juger autrement. Par conséquent, la Chambre Contentieuse constate qu'il n'y a **aucune violation** du Chapitre V du RGPD.

[24] Lignes directrices du Groupe 29 concernant les délégués à la protection des données 16/FR WP 243.

II.11. Registre des activités de traitement (article 30 du RGPD) vis-à-vis de la première défenderesse

II.11.1. Constatations du Service d'Inspection

134. Le Service d'Inspection constate que le registre des activités de traitement fourni est postérieur au premier contact avec le Service d'Inspection. Le Service d'Inspection en arrive à cette conclusion sur la base des éléments suivants. Le registre des activités de traitement mentionne l'adresse e-mail dataprotection@benepack.com comme adresse de contact du responsable du traitement. Toutefois, cette adresse n'a été créée qu'après le premier contact avec le Service d'Inspection. Étant donné que la première défenderesse indique au cours de l'enquête d'inspection qu'il s'agit de la seule version du registre des activités de traitement, le Service d'Inspection conclut que la première défenderesse ne disposait pas d'un registre des activités de traitement avant l'enquête d'inspection. Le Service d'Inspection constate qu'il s'agit d'une violation de l'article 30 du RGPD, car la première défenderesse doit tenir un registre des activités de traitement au moins pour les traitements concernant son personnel. En effet, les traitements ne peuvent pas être considérées comme occasionnels au sens de l'article 30.5 du RGPD. En outre, le Service d'Inspection relève que la première défenderesse traite des catégories particulières de données à caractère personnel et des données pénales.

135. De plus, selon les constatations du Service d'Inspection, le registre des activités de traitement est lacunaire en plusieurs points. Le CEO et le gestionnaire des ressources humaines de la première défenderesse sont présentés comme délégués à la protection des données (article 30.1.a) du RGPD). Les finalités de traitement figurant dans le registre des activités de traitement diffèrent sur plusieurs points des finalités de traitement reprises pour ces traitements dans le règlement de travail (version juin 2022) (article 30.1.b) du RGPD). Les dix catégories de données à caractère personnel qui figurent dans le règlement de travail (version juin 2022) ne sont pas ou pas entièrement reprises dans le registre des activités de traitement (article 30..1.c) du RGPD) et des collaborateurs internes sont présentés comme des sous-traitants alors que, par exemple, le sous-traitant pour le système d'enregistrement biométrique du temps n'est pas mentionné (article 30.1.d) du RGPD).

II.11.2. Évaluation par la Chambre Contentieuse

136. Aux termes de l'article 30 du RGPD, tout responsable du traitement doit tenir un registre des activités de traitement effectuées sous sa responsabilité. L'article 30.1.a) à g) inclus du RGPD dispose qu'en ce qui concerne les traitements effectués en qualité de responsable du traitement, les informations suivantes doivent être disponibles :

a) le nom et les coordonnées du responsable du traitement et des éventuels responsables conjoints du traitement et, le cas échéant, du représentant du responsable du traitement et du délégué à la protection des données ;

b) les finalités du traitement ;

c) une description des catégories de personnes concernées et des catégories de données à caractère personnel ;

d) les catégories de destinataires auxquels les données à caractère personnel ont été ou seront communiquées, y compris les destinataires dans des pays tiers ou des organisations internationales ;

e) le cas échéant, les transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale, y compris l'identification de ce pays tiers ou de cette organisation internationale et, dans le cas des transferts visés à l'article 49, paragraphe 1, deuxième alinéa du RGPD, les documents attestant de l'existence de garanties appropriées ;

f) dans la mesure du possible, les délais prévus pour l'effacement des différentes catégories de données ;

g) dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles visées à l'article 32.1 du RGPD.

137. En ce qui concerne le nom et les coordonnées du délégué à la protection des données (article 30.1.a) du RGPD), la Chambre Contentieuse constate, conformément au rapport d'inspection, que le registre des activités de traitement mentionne effectivement les coordonnées du CEO et du gestionnaire des ressources humaines en tant que délégués à la protection des données.

138. En ce qui concerne les finalités du traitement (article 30.1.b) du RGPD), la Chambre Contentieuse constate que les finalités mentionnées dans le registre des activités de traitement ne correspondent pas aux finalités énumérées dans le règlement de travail (version juin 2022). Le registre des activités de traitement mentionne en tant que finalité de traitement pour les empreintes digitales : "sont enregistrées pour l'enregistrement du temps. Au début et à la fin de la journée de travail, les travailleurs doivent pointer leur entrée et leur sortie à l'aide de leurs empreintes digitales". Le règlement de travail (version juin 2022) mentionne non seulement l'enregistrement du temps de travail, mais aussi la lutte contre la fraude et la sécurité du personnel. En ce qui concerne les caméras de surveillance également, la Chambre Contentieuse relève une discordance entre les finalités du traitement. Le registre des activités de traitement met en avant "la sécurité et la santé", tandis que le règlement de travail (juin 2022) met l'accent sur "le contrôle sur le lieu de travail : pour garantir la sécurité de l'ensemble du personnel, lutter contre les éventuelles fraudes,

les infractions et les violations potentielles par des tiers ; et la protection des actifs de l'entreprise" comme finalités de traitement.

139. En ce qui concerne les catégories de données à caractère personnel (article 30.1.c) du RGPD), la Chambre Contentieuse constate que le règlement de travail mentionne plusieurs catégories de données à caractère personnel traitées, qui ne sont pas reprises dans le registre des activités de traitement. Il s'agit des catégories suivantes : coordonnées des personnes à éventuellement contacter en cas d'urgence, fonction actuelle (et précédente) des personnes employées auprès de la première défenderesse, primes et avantages salariaux, biens de l'entreprise en possession de la personne concernée (téléphone portable, voiture de fonction, ordinateur portable, etc.), informations concernant la personne concernée dans le cadre de la gestion des prestations, de l'apprentissage et du développement, de la santé au travail et des accidents du travail, informations fournies par la personne concernée ou relatives à la personne concernée dans le cadre de la procédure interne de dénonciation et enfin, les informations concernant certaines infractions, par exemple les accidents de la route susceptibles d'engager la responsabilité de la personne concernée ou de la première défenderesse. Les catégories "enregistrements d'images au moyen de caméras de surveillance et informations fournies par la personne concernée ou relatives à la personne concernée dans le cadre des comptes de pension, des pensions, de l'assurance hospitalisation et d'autres informations sur les prestations" sont reprises de manière incomplète dans le registre des activités de traitement.

140. Enfin, la Chambre Contentieuse constate que la deuxième défenderesse, en sa qualité de sous-traitant dans le cadre du système biométrique d'enregistrement du temps, n'est pas mentionnée en tant que destinataire dans le registre des activités de traitement (article 30.1.d) du RGPD).

141. Afin de pouvoir appliquer efficacement les obligations contenues dans le RGPD, il est essentiel que le responsable du traitement (et les sous-traitants) ai(en)t un aperçu des traitements de données à caractère personnel qu'il(s) effectue(nt). Ce registre constitue dès lors en premier lieu un instrument pour aider le responsable du traitement à respecter le RGPD pour les différents traitements de données qu'il réalise. La Chambre Contentieuse estime que le registre des activités de traitement est un instrument essentiel dans le cadre du principe de responsabilité déjà mentionné (article 5.2 et article 24.1 du RGPD) et que ce registre est à la base de toutes les obligations imposées par le RGPD au responsable du traitement. Il importe dès lors que ce registre soit complet et exact.

142. La Chambre Contentieuse estime que le registre des activités de traitement qui a été transmis par la première défenderesse est incomplet et partiellement inexact, comme cela est constaté dans le rapport d'inspection. Dans ce cadre, la Chambre Contentieuse fait remarquer que, bien que la première défenderesse entreprenne effectivement des

démarches actuellement pour rectifier ces violations, trop peu d'efforts ont été fournis pour mettre au point le registre des activités de traitement selon les dispositions de l'article 30 du RGPD. La Chambre Contentieuse estime **donc qu'il y a violation de l'article 30.1.a), b), c), d) du RGPD.**

II.12. Responsabilité (article 5.2 du RGPD) de la première défenderesse

143. La Chambre Contentieuse rappelle que chaque responsable du traitement doit respecter les principes de base de la protection des données à caractère personnel, tels que définis à l'article 5.1 du RGPD, et doit être en mesure de démontrer le respect de ces principes. Cela découle du principe de responsabilité repris à l'article 5.2 du RGPD *juncto* l'article 24.1 du RGPD, tel que confirmé par la Chambre Contentieuse.[25]

144. En vertu des articles 24 et 25 du RGPD, le responsable du traitement doit prendre des mesures techniques et organisationnelles appropriées pour s'assurer et être en mesure de démontrer que le traitement est effectué conformément au RGPD. Dans ce cadre, il doit appliquer efficacement les principes de protection des données, protéger les droits des personnes concernées et traiter uniquement les données à caractère personnel qui sont nécessaires à chaque finalité spécifique du traitement.

145. Dans le cadre de son enquête, le Service d'Inspection a évalué dans quelle mesure la première défenderesse a pris les mesures techniques et organisationnelles nécessaires pour satisfaire à ces principes de l'article 5.1 du RGPD et en particulier les principes de licéité et de transparence, de limitation des finalités, de minimisation des données et de limitation de la conservation (voir les points II.1 à II.6).

146. En outre, la Chambre Contentieuse constate que la description au point II.8 des mesures de sécurité prises ne montre pas comment un contrôle adéquat de ces mesures est organisé, ni ne précise dans quelle mesure la première défenderesse vérifie si les mesures sont efficaces et à quelle fréquence cela est vérifié. Enfin, aucune politique n'a été mise en place pour la gestion efficace des incidents de sécurité de l'information. La Chambre Contentieuse estime que la nature sensible des données biométriques traitées à grande échelle par la première défenderesse aurait dû l'inciter bien plus tôt à mieux se conformer aux principes susmentionnés du RGPD (dont la sécurité des données), notamment en anticipant les risques inhérents à de telles violations.

147. Il ressort de ce qui précède que les mesures techniques et organisationnelles prises suite à l'installation et la mise en service du système d'enregistrement du temps au moyen de données biométriques n'étaient pas appropriées pour assurer le respect des principes fondamentaux du RGPD, et plus particulièrement des principes de licéité, de limitation des

---

[25] Décision quant au fond 34/2020 du 23 juin 2020, disponible via le lien suivant : https://www.autoriteprotectiondonnees.be/professionnel/publications/decisions.

finalités, de transparence et de minimisation des données. En tant que responsable du traitement, la première défenderesse n'a pas pris de mesure appropriée, ou de mesures appropriées suffisantes, pour garantir et démontrer que le traitement litigieux a été effectué conformément au RGPD, ce qui entraîne une **violation de l'article 5.2 du RGPD.**

II.13. L'article 28.3 du RGPD vis-à-vis de la deuxième défenderesse

II.13.1. Constatations dans le rapport d'inspection

148. Le Service d'Inspection constate dans son rapport que le contrat de sous-traitance entre la première et la deuxième défenderesse ne répond pas aux exigences de l'article 28.3 du RGPD, vu qu'il ne contiendrait qu'une description des mesures générales de sécurité, et non une description détaillée axée sur les exigences élevées de sécurité lors du traitement de données biométriques. Selon le Service d'Inspection, le contrat de sous-traitance proprement dit reprend d'une part les dispositions légales de l'article 32.1 du RGPD et se réfère à l'annexe pour plus de détails. Selon le Service d'Inspection, cette annexe B contient une description concrète, mais encore succincte et insuffisamment adaptée à la nature spécifique des données traitées. Cette généralité et le degré limité de détail de l'annexe B ne permettent pas de déterminer, par exemple, le niveau de cryptage appliqué aux données biométriques brutes ou conservées comme gabarit, l'utilisation d'une fonction de vérification ou d'une fonction d'identification dans la phase de comparaison du processus d'authentification biométrique, le système utilisé par le sous-traitant pour l'effacement et la destruction des données biométriques après l'expiration du délai de conservation, et les modalités précises des politiques d'accès logiques et physiques appliquées par le sous-traitant.

149. Selon le rapport d'inspection, le contrat de sous-traitance présente également des lacunes en ce qui concerne la définition de la nature et de la finalité du traitement et du type de données à caractère personnel traitées, exigée par l'article 28.3 du RGPD.

150. En ce qui concerne la nature et la finalité du traitement, le Service d'Inspection constate qu'il est impossible de les vérifier sur la base des dispositions du contrat de sous-traitance. La seule finalité à déduire est l'exécution du contrat de services entre les deux défenderesses. Du contrat de services proprement dit, le Service d'Inspection peut tout au plus déduire le traitement des empreintes digitales et des données d'enregistrement du temps de travail des travailleurs. Le contrat de sous-traitance ne permet pas au Service d'Inspection de clarifier le type de données à caractère personnel traitées par la deuxième défenderesse pour le compte de la première défenderesse. Le contrat ne contient qu'un menu déroulant ouvert ainsi que 20 champs à compléter librement par le client. Le client n'a pas non plus indiqué de choix de catégories à traiter.

151. Le Service d'Inspection attache une importance particulière au rôle du sous-traitant dans l'accomplissement de cette obligation conjointe en vertu de l'article 28.3 du RGPD parce que le sous-traitant est la seule des deux parties à posséder les connaissances techniques qui permettent une description complète du traitement. Sans cette description complète, ni le responsable du traitement ni l'autorité de contrôle ne peuvent évaluer correctement le contenu et les risques du traitement confié au sous-traitant.

152. Le Service d'Inspection constate que, même à sa demande explicite, le sous-traitant (la deuxième défenderesse) n'est pas en mesure de fournir une description technique complète du traitement qui lui est confié. Ceci ressort de sa réponse minimaliste à la question du Service d'Inspection sur le fonctionnement du système d'enregistrement du temps. Ensuite, la deuxième défenderesse semble ne pas pouvoir fournir d'informations supplémentaires sur certains éléments tels que : le cryptage des données biométriques brutes et des gabarits, la présence d'un contrôle d'intégrité lié aux données biométriques, les modalités techniques précises de la phase de collecte et de comparaison du processus d'authentification biométrique et la technique utilisée pour l'effacement et la destruction des données après l'expiration du délai de conservation.

153. Dans son rapport, le Service d'Inspection se réfère également au paragraphe 103 des lignes directrices 07/2020 de l'EDPB *concernant les notions de responsable du traitement et de sous-traitant dans le RGPD*[26], qui dispose que tant le responsable du traitement que le sous-traitant sont chargés de veiller à ce qu'un contrat ou un autre acte juridique régisse le traitement. L'autorité de contrôle compétente peut infliger une amende administrative aussi bien au responsable du traitement qu'au sous-traitant, en tenant compte de l'article 83 du RGPD et des circonstances propres à chaque situation. Les contrats conclus avant la date d'entrée en vigueur du RGPD auraient dû être adaptés dans le sens de l'article 28.3 du RGPD. Ne pas l'avoir fait constitue une violation de la disposition en question.

154. Enfin, selon le Service d'Inspection, la deuxième défenderesse remet en cause la qualification juridique en tant que données biométrique des données à caractère personnel qu'elle traite (dans le cadre du traitement litigieux). Or, le contrat de sous-traitance fait référence aux gabarits biométriques des données à caractère personnel traitées par la deuxième défenderesse. Le Service d'Inspection n'est pas d'accord avec cette déclaration. Dès lors, le Service d'Inspection a des doutes quant aux mesures techniques et organisationnelles prises par la deuxième défenderesse, puisqu'en vertu de l'article 32.1 du RGPD, elles doivent être appropriées au risque du traitement qui a apparemment été mal évalué par la deuxième défenderesse.

---

[26] Lignes directrices 07/2020 *concernant les notions de responsable du traitement et de sous-traitant dans le RGPD*, version 2.0, adoptées par l'EDPB le 7 juillet 2021, consultables via le lien suivant : https://www.edpb.europa.eu/system/files/2023-10/edpb_guidelines_202007_controllerprocessor_final_fr.pdf.

155. Le Service d'Inspection conclut donc que le contrat de sous-traitance n'est pas conforme à l'article 28.3 du RGPD en ce qu'il ne répond pas aux exigences minimales de cette disposition, notamment la définition de la nature et de la finalité du traitement, le type de données à caractère personnel et les mesures techniques et organisationnelles appliquées par le sous-traitant.

II.13.2. Position de la deuxième défenderesse

156. Dans ses conclusions, la deuxième défenderesse argumente qu'elle a bien la capacité de partager les connaissances appropriées sur le système. Elle a fourni les informations pertinentes à la première défenderesse en temps opportun. Lors de la conclusion du contrat, la première défenderesse disposait d'une documentation et d'informations détaillées dans le contrat de sous-traitance et avait accès à la plate-forme en ligne, et elle a également reçu plusieurs formations. En outre, c'est la première défenderesse qui enregistre les personnes dans le système. Le traitement de données à caractère personnel a donc débuté dès que la première défenderesse a commencé cet enregistrement. Par conséquent, la première défenderesse a pu prendre connaissance de toutes les informations disponibles concernant les processus avant d'entamer le traitement. En ce qui concerne sa réponse minimaliste au Service d'Inspection, la deuxième défenderesse fait remarquer qu'immédiatement après l'avoir interrogée une première fois, le Service d'Inspection a clôturé l'enquête et a préparé le rapport d'inspection ; or, la première défenderesse a été interrogée plus d'une fois.

157. En outre, la deuxième défenderesse objecte que le Service d'Inspection a constitué un dossier incomplet. Le Service d'Inspection a uniquement demandé à la première défenderesse le contrat de sous-traitance, que la première défenderesse lui a fourni, mais sans le Z IT Guide. Ce Z IT Guide fait intégralement partie, en tant qu'annexe, du contrat de sous-traitance. La deuxième défenderesse n'était pas au courant qu'un contrat de sous-traitance incomplet avait été communiqué, et aucune question ne lui a été posée à ce sujet. En outre, la deuxième défenderesse dénonce le fait que le Service d'Inspection l'a interrogée non seulement sur les traitements qui lui ont été confiés, mais aussi sur les tâches et les traitements de la première défenderesse. La deuxième défenderesse argumente que le Service d'Inspection lui reproche, quant au caractère incomplet de sa réponse (*quod non,* selon la deuxième défenderesse), de ne pas donner une description technique complète des traitements effectués par la première défenderesse, ce qu'elle n'est pas tenue de faire. La référence par le Service d'Inspection au paragraphe 103 des lignes directrices 07/2020 n'a été adoptée qu'en juillet 2021, ce paragraphe n'était donc pas encore présent dans la version 2020. À cet égard, il est important de souligner que le contrat de sous-traitance a été conclu le 14 février 2020. Dès lors, un défaut de réponse de la première défenderesse, pour autant qu'il ait déjà été constaté, ne peut pas être imputé à la deuxième défenderesse mais le Service d'Inspection doit interroger la première défenderesse à ce sujet.

158. Par ailleurs, la deuxième défenderesse relève qu'il lui est reproché de ne pas avoir fourni d'informations sur la technique utilisée pour l'effacement et la destruction (par exemple, l'écrasement, la démagnétisation, l'effacement cryptographique, etc.) des données après l'expiration du délai de conservation, en citant la recommandation 03/2020 de l'APD. Le Service d'Inspection est parvenu à cette conclusion à la suite d'une réponse de la deuxième défenderesse à la question "*Quel est le système utilisé pour l'effacement et la destruction des données/gabarits biométriques après l'expiration du délai de conservation ? Qui est responsable de cet effacement [première défenderesse] ou [deuxième défenderesse] ?*". La deuxième défenderesse a répondu qu'aucune donnée biométrique brute n'était conservée. Les modèles cryptés sont stockés sur le terminal ST25 et dans la base de données SQL cloud tant que le travailleur existe dans la base de données SQL cloud. La distribution sur un terminal ou plusieurs terminaux ST25 est effectuée sur la base de la configuration dans l'application web T&A de Z. La deuxième défenderesse constate que cette réponse n'a apparemment pas été considérée comme concluante par le Service d'Inspection. La deuxième défenderesse fait observer que le Service d'Inspection aurait pu poser une question complémentaire à ce sujet, s'il jugeait que la réponse donnée était insuffisante.

159. La qualification juridique des données traitées par le sous-traitant est un point de discorde entre la deuxième défenderesse et le Service d'Inspection. La deuxième défenderesse estime qu'avec Z, elle ne traite pas de données biométriques ni aucune autre catégorie particulière de données à caractère personnel. La deuxième défenderesse fait observer que les données biométriques (article 4.14 du RGPD) ne constituent une catégorie particulière en vertu de l'article 9 du RGPD que si elles sont traitées en vue d'une identification unique. La deuxième défenderesse affirme qu'aucune comparaison n'est effectuée sur la plate-forme en ligne qu'elle met à disposition. La comparaison des données biométriques intervient uniquement dans le lecteur spécifique, qui est lié aux terminaux chez le client, dans le cas présent la première défenderesse. Seul le lecteur, en tant que module séparé, contient un logiciel propre à l'entreprise avec des algorithmes secrets dont le fonctionnement n'est connu que du fournisseur du module ; la technologie utilisée constitue un secret commercial. Le fabricant ne révèle pas comment les gabarits sont créés, ni quelle clé est utilisée pour le cryptage. Le fabriquant confirme néanmoins qu'ils ne sont jamais divulgués. La deuxième défenderesse ajoute qu'il est impossible pour quiconque d'utiliser les données fournies par le lecteur biométrique pour identifier une personne lors de l'enregistrement d'un utilisateur. La seule chose que permet le fichier est de le retransmettre à un lecteur du même fabricant au sein du système dans le but d'obtenir comme réponse la vérification d'une identité (*match* ou *no match*). Ainsi, la seule réponse qu'un lecteur donnera est une correspondance avec un identifiant connu ou une absence de correspondance. Toute personne qui parviendrait à obtenir illégalement le fichier crypté de données du lecteur biométrique après

l'enregistrement d'un utilisateur ne pourrait utiliser ce fichier dans aucun autre type d'outil biométrique, car elle ne disposerait pas de la ou des clé(s) unique(s). Par conséquent, la deuxième défenderesse conclut qu'elle offre un système de stockage en ligne, mais ne choisit pas quels terminaux sur place chez la première défenderesse stockent certaines données liées à la biométrie, et n'organise certainement pas la phase de comparaison sur sa propre plate-forme (en ligne). Elle n'est que le prestataire de services de conservation d'un fichier dont personne ne peut obtenir le décryptage sans pirater le lecteur du fabricant.

160. La deuxième défenderesse fait également valoir qu'il lui est raisonnablement impossible d'obtenir les informations de décryptage, ce qui soulève la question de savoir si les fichiers constituent effectivement des données à caractère personnel au sens de l'article 4.14 du RGPD.

II.13.3. Évaluation par la Chambre Contentieuse

161. Tout traitement de données à caractère personnel par un sous-traitant doit être régi par un contrat ou un autre acte juridique en vertu du droit de l'UE ou d'un État membre entre le responsable du traitement et le sous-traitant, comme l'exige l'article 28.3 du RGPD.

162. Le Service d'Inspection constate plusieurs violations de l'article 28.3 du RGPD : (i) le contrat de sous-traitance entre la première défenderesse en tant que responsable du traitement et la deuxième défenderesse en tant que sous-traitant n'est pas conforme aux exigences de l'article 28.3 du RGPD, en particulier en ce qui concerne les exigences minimales de relatives à la définition de la nature et de la finalité du traitement, le type de données à caractère personnel et les mesures techniques et organisationnelles appliquées par le sous-traitant ; (iii) la deuxième défenderesse ne satisfait pas aux obligations en vertu de l'article 28.3 du RGPD compte tenu du fait qu'alors qu'elle était la seule à avoir les connaissances techniques du système, elle aurait néanmoins insuffisamment définit le traitement et enfin, elle aurait remis en cause la qualification juridique des données biométriques.

(i) Description de la nature et de la finalité du traitement, du type de données à caractère personnel et des mesures techniques et organisationnelles appliquées

163. Premièrement, la Chambre Contentieuse examine dans quelle mesure le contrat de sous-traitance entre la première défenderesse en tant que responsable du traitement et la deuxième défenderesse en tant que sous-traitant répond aux exigences de l'article 28.3 du RGPD, en particulier en ce qui concerne les exigences minimales relatives à la définition de la nature et de la finalité du traitement, du type de données à caractère personnel et des mesures techniques et organisationnelles appliquées par le sous-traitant. [27]

[27] Voir constatation 12 du rapport d'inspection.

164. La Chambre Contentieuse constate que le contrat de sous-traitance se compose de plusieurs parties, comme indiqué dans les conclusions de la deuxième défenderesse, à savoir le contrat principal proprement dit avec 2 annexes (Enclosure 1 et Enclosure 2). L'Enclosure 2 du contrat principal comporte également 2 annexes, à savoir l'Attachment 1 : "Z IT Guide" et l'Attachment 2 "*Data processing agreement*", comportant à nouveau 3 annexes : *Attachment A (description of the processing), Attachment B (technical and organizational security measures) et Attachment C (subprocessors)*.

165. Se référant aux lignes directrices 07/2020 concernant les notions de "responsable du traitement" et de "sous-traitant" dans le RGPD[28], la Chambre Contentieuse rappelle que le contrat de sous-traitance doit reprendre entre autres les éléments suivants : une description du type de données à caractère personnel et des catégories de personnes concernées ainsi que la nature du traitement. En ce qui concerne la nature et la finalité du traitement, l'EDPB précise que cette description devrait être aussi complète que possible, selon l'activité de traitement concernée, de manière à permettre à des parties externes (par exemple, des autorités de contrôle) de comprendre le contenu et les risques du traitement confié au sous-traitant.[29] La "*desciption of the processing*" telle que reprise dans l' *Attachment 2* du contrat de sous-traitance dispose que le contrat porte sur la conservation de différentes catégories de données à caractère personnel et de données sensibles. Le contrat de sous-traitance et toutes ses annexes permet de déduire indirectement qu'il est question du traitement des empreintes digitales et de l'enregistrement du temps des travailleurs, notamment à partir de l'Enclosure 1 du contrat de sous-traitance qui mentionne des *Fingerprint licenses* (licences d'empreintes digitales) et indique que toutes les informations apportées par le client (en l'espèce, le responsable du traitement) en rapport avec l'enregistrement du temps seront stockées dans la base de données de Z pendant une période déterminée.

166. D'après l'EDPB, les types de données à caractère personnel devraient être précisés de la manière la plus détaillée possible. Se contenter d'indiquer qu'il s'agit de données à caractère personnel au sens de l'article 4.1 du RGPD ou de catégories particulières de données à caractère personnel au sens de l'article 9 du RGPD ne suffirait pas.[30] La Chambre Contentieuse constate que le contrat de sous-traitance repris dans l'*Enclosure* 2 "*Description of the processing*" laisse la possibilité d'indiquer quelles données à caractère

---

[28] Lignes directrices 07/2020 *concernant les notions de responsable du traitement et de sous-traitant dans le RGPD*, version 2.0, adoptées par l'EDPB le 7 juillet 2021, consultable via le lien suivant : https://www.edpb.europa.eu/system/files/2023-10/edpb_guidelines_202007_controllerprocessor_final_fr.pdf.

[29] Lignes directrices 07/2020 *concernant les notions de responsable du traitement et de sous-traitant dans le RGPD*, version 2.0, adoptées par l'EDPB le 7 juillet 2021, para. 114, consultables via le lien suivant : https://www.edpb.europa.eu/system/files/2023-10/edpb_guidelines_202007_controllerprocessor_final_fr.pdf.

[30] Lignes directrices 07/2020 concernant les notions de responsable du traitement et de sous-traitant dans le RGPD, version 2.0, adoptées par l'EDPB le 7 juillet 2021, para. 114, consultables via le lien suivant : https://www.edpb.europa.eu/system/files/2023-10/edpb_guidelines_202007_controllerprocessor_final_fr.pdf.

personnel seront spécifiquement traitées sur la base du contrat de sous-traitance ["*Please select the categories you intend to use with the Services*"]. Parmi celles-ci, le contrat de sous-traitance prévoit également quatre catégories de données à caractère personnel particulières traitées par la deuxième défenderesse sur la base de du contrat de sous-traitance. Ici aussi, il est demandé d'indiquer les catégories pertinentes ["*Please select the categories you intend to use with the services*"]. La Chambre Contentieuse constate que les catégories pertinentes n'ont été indiquées ni pour les données à caractère personnel, ni pour les données à caractère personnel particulières. La Chambre Contentieuse constate que cette violation n'a été reprochée par le Service d'Inspection qu'à la deuxième défenderesse alors que les obligations de l'article 28.3 du RGPD incombent aux deux parties contractantes. Néanmoins, l'absence de désignation pourrait également être imputée à la première défenderesse puisque, en tant que responsable du traitement, elle détermine les finalités et les moyens du traitement.

167. En conclusion, la Chambre Contentieuse constate que les informations requises en vertu de l'article 28.3., paragraphe 1 (la nature et la finalité du traitement et le type de données à caractère personnel) peuvent être déduites de la lecture intégrale du contrat de sous-traitance, mais qu'il est recommandé, par souci de clarté, que les (catégories de) données à caractère personnel traitées, particulières ou non, soient indiquées dans l'annexe comme prévu.

168. Le Service d'Inspection a également constaté dans son rapport qu'il est question d'une violation de l'article 28.3.c) du RGPD, vu le caractère général et le degré limité de détail dans l'énumération des mesures techniques et organisationnelles appliquées.

169. L'article 28.3.c) du RGPD exige que toutes les mesures de sécurité requises en vertu de l'article 32 du RGPD soient reflétées dans le contrat de sous-traitance. Ce contrat de sous-traitance ne peut pas simplement répéter les dispositions du RGPD mais doit contenir des informations sur les mesures de sécurité ou des références à ces mesures. Le niveau de détail doit permettre au responsable du traitement d'évaluer l'adéquation des mesures conformément à l'article 32.1 du RGPD.[31]

170. L'article 32.2 du RGPD dispose que lors de l'évaluation du niveau de sécurité approprié, il faut tenir compte 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. À cet égard, il convient donc de tenir également compte de la nature particulière ou non des données à caractère

[31] Lignes directrices 07/2020 concernant les notions de responsable du traitement et de sous-traitant dans le RGPD, version 2.0, adoptées par l'EDPB le 7 juillet 2021, para. 126, consultables via le lien suivant : https://www.edpb.europa.eu/system/files/2023-10/edpb_guidelines_202007_controllerprocessor_final_fr.pdf.

personnel traitées, ce qui constitue un point de désaccord entre le Service d'Inspection et la deuxième défenderesse.

171. En ce qui concerne la qualification des données à caractère personnel traitées par la deuxième défenderesse, la Chambre Contentieuse rappelle la définition des données biométriques et le traitement d'une éventuelle catégorie particulière de données à caractère personnel. Comme l'indique également la deuxième défenderesse dans ses conclusions, les données biométriques ne constituent pas d'emblée une catégorie particulière de données à caractère personnel au sens de l'article 9 du RGPD. Pour ce faire, la finalité de l'identification unique est requise. Comme déjà indiqué, la finalité d'identification est présente dans le chef de la première défenderesse en tant que responsable du traitement dans le cadre de l'enregistrement du temps, mais pas dans le chef de la deuxième défenderesse. Cette dernière reçoit de la première défenderesse des données qu'elle traite (c'est-à-dire qu'elle stocke) sans finalité d'identification ou d'authentification, de sorte qu'il n'est pas question de traitement de données à caractère personnel particulières au sens de l'article 9 du RGPD. Les mesures de sécurité applicables doivent dès lors être adaptées en conséquence.

172. Comme déjà expliqué, le contrat de sous-traitance se compose du contrat principal et de 2 annexes (Attachment 1 et Attachment 2). Comme l'a également indiqué la deuxième défenderesse, la Chambre Contentieuse observe que le Z IT Guide (Attachment 2) manquait au dossier d'Inspection, de sorte qu'il n'a pas été pris en compte au cours de l'enquête.

173. Ce Z IT Guide explique en 13 pages les aspects liés à la sécurité de l'application Z, en reprenant des informations concrètes sur les mesures de sécurité prises pour les traitements qui lui sont confiés, à savoir le stockage des données dans Z. Ce guide contient des informations sur les serveurs sur lesquels les données sont stockées, les mesures de sécurité (telles que les systèmes anti-virus, les pare-feu, les certificats SSL et les services de monitoring). La Chambre Contentieuse estime que le degré de détail de la description des mesures de sécurité répond aux exigences imposées par l'article 28.3.c) RGPD.

> *(ii) la deuxième défenderesse ne satisfait pas aux obligations en vertu de l'article 28.3 du RGPD compte tenu du fait qu'alors qu'elle était la seule à avoir les connaissances techniques du système, elle aurait néanmoins insuffisamment définit le traitement et enfin, elle aurait remis en cause la qualification juridique des données biométriques.*

174. La Chambre Contentieuse observe que ces constatations ne portent pas sur le contenu du contrat de sous-traitance tel que défini à l'article 28.3 du RGPD, mais plutôt sur les échanges d'informations précontractuelles avec la première défenderesse (par exemple sur la base de l'article 28.1 du RGPD) ou sur le principe de responsabilité en vertu de l'article 5.2 du RGPD.

175. En ce qui concerne la constatation selon laquelle la deuxième défenderesse n'aurait pas suffisamment décrit le traitement, la Chambre Contentieuse renvoie au point II.7 où elle constate que le contrat de sous-traitance n'a pas été communiqué dans son intégralité au Service d'Inspection par la première défenderesse. Il n'a pas été demandé à la deuxième défenderesse de transmettre le contrat de sous-traitance au Service d'Inspection.

176. Comme expliqué, le Z IT Guide contient des informations sur les connaissances techniques du système. La deuxième défenderesse a transféré toutes ces informations à la première défenderesse, responsable du traitement, sur la base desquelles cette dernière a pu effectuer l'analyse requise en la matière (voir point II.8). En outre, la deuxième défenderesse a également proposé une formation sur le fonctionnement de Z. Par ailleurs, la Chambre Contentieuse note que de la documentation supplémentaire, un portail et une fonction d'aide étaient également disponibles en ligne, ainsi qu'un helpdesk. Comme le fait également valoir la deuxième défenderesse, l'enregistrement des travailleurs ne débute qu'au moment où la première défenderesse l'active. Par conséquent, elle pouvait demander des informations supplémentaires si nécessaire avant de commencer l'enregistrement du temps. La Chambre Contentieuse estime dès lors que le traitement est suffisamment décrit et que la deuxième défenderesse a fourni les informations nécessaires à la première défenderesse.

177. Le Service d'Inspection constate également que, même sur demande explicite du Service d'Inspection, la deuxième défenderesse n'est pas en mesure de fournir une description technique complète du traitement qui lui est confié. À cet égard, le Service d'Inspection se réfère aux réponses minimalistes de la deuxième défenderesse et à son incapacité à fournir des informations supplémentaires sur certains éléments.

178. La Chambre Contentieuse relève tout d'abord qu'une éventuelle réponse minimaliste au Service d'Inspection deux ans après la conclusion du contrat de sous-traitance n'a aucune incidence sur le respect correct ou non de l'article 28.3 du RGPD, qui ne définit que les exigences de contenu du contrat de sous-traitance.

179. La Chambre Contentieuse relève en outre que, dans sa lettre du 6 juillet 2022, le Service d'Inspection a demandé à la deuxième défenderesse d'expliquer le fonctionnement technique du système et, en particulier, la manière dont les données biométriques collectées par le biais du système sont traitées. À cette occasion, le Service d'Inspection demande que cette explication soit accompagnée d'un aperçu aussi schématique que possible des différentes étapes du traitement, de la collecte à l'effacement. Par ailleurs, le Service d'Inspection demande de préciser quelles mesures de sécurité techniques et organisationnelles sont prises par la deuxième défenderesse pour protéger l'intégrité, la disponibilité et la confidentialité des données, alors que c'est en fait à la première défenderesse que ces obligations incombent. Ensuite, le Service d'Inspection a posé

12 questions supplémentaires. Ces questions concernent également les différentes phases de l'enregistrement du temps.

180. La Chambre Contentieuse constate que la deuxième défenderesse a répondu aux 12 questions mais n'a pas pu répondre à toutes les questions sur le fond. Certaines informations ne sont en effet pas connues de la deuxième défenderesse, étant donné qu'elle n'est pas responsable du traitement pour toute la chaîne des traitements dans le cadre de l'enregistrement du temps en question. La deuxième défenderesse a formulé une réponse aux questions qui concernaient les traitements qui lui avaient été confiés en sa qualité de sous-traitant. À cet égard, la deuxième défenderesse a également indiqué pourquoi elle ne pouvait pas répondre aux autres questions, par exemple parce qu'elle ne traitait pas certains aspects de la chaîne d'enregistrement du temps.

181. Au vu de ce qui précède, la Chambre Contentieuse conclut qu'**il n'y a pas de violation de l'article 28.3 du RGPD dans le chef de la deuxième défenderesse.**

II.14. Délégué à la protection des données (article 37.1, b) et c) du RGPD) vis-à-vis de la deuxième défenderesse

II.14.1. Constatations dans le rapport d'inspection

182. Le Service d'Inspection constate dans le rapport d'inspection que la deuxième défenderesse ne respecte pas les obligations relatives à la désignation d'un délégué à la protection des données au sens de l'article 37.1.b) et c) du RGPD. En premier lieu, le Service d'Inspection déclare que les exigences relatives à la désignation d'un délégué à la protection des données au sens de l'article 37.1.c) du RGPD sont remplies étant donné qu'elle traite des données biométriques, que le traitement est effectué à grande échelle et qu'elle en est la principale responsable. Par conséquent, le Service d'Inspection conclut qu'un délégué à la protection des données aurait dû être désigné.

183. Premièrement, le Service d'Inspection ne partage pas le point de vue de la deuxième défenderesse concernant le fait qu'elle ne traiterait pas de données biométriques (voir le point II.13). Ensuite, le Service d'Inspection se réfère à la clause standard dans l'annexe A du contrat de sous-traitance dans laquelle, en tant que sous-traitant, la deuxième défenderesse s'ouvre également au traitement d'autres catégories de données à caractère personnel. Deuxièmement, en ce qui concerne le caractère à grande échelle du traitement, le Service d'Inspection constate qu'il ressort du rapport du conseil d'administration de la deuxième défenderesse que Z est distribué dans 9 pays européens, ce qui permet au Service d'Inspection de comprendre qu'il est question d'une grande couverture géographique. Le Service d'Inspection déclare qu'il n'a aucune idée du nombre de personnes concernées ou de la quantité de données traitées, mais relève en outre que la durée et la permanence du traitement des données inhérentes à un système d'enregistrement du temps de travail

constitue un élément supplémentaire dans l'évaluation de la nature à grande échelle du traitement. Troisièmement, en ce qui concerne le critère du caractère principal, le Service d'Inspection déclare qu'il est clair que le traitement de données constitue une activité principale de l'entreprise et non une fonction de soutien nécessaire à l'activité principale de l'organisation.

184. Enfin, le Service d'Inspection fait observer que l'on peut également considérer sur la base de l'article 37.1.b) du RGPD que la deuxième défenderesse est tenue de désigner un délégué à la protection des données puisque l'enregistrement quotidien des heures d'arrivée et de départ des travailleurs sur un lieu de travail déterminé constitue une observation régulière et systématique des personnes concernées.

II.14.2. Position de la deuxième défenderesse

185. La deuxième défenderesse fait valoir dans ses conclusions qu'elle n'est nullement obligée de désigner un délégué à la protection des données, que ce soit sur la base de l'article 37.1.c) du RGPD ou sur la base de l'article 37.1.b) du RGPD.

186. En ce qui concerne l'applicabilité de l'article 37.1.c) du RGPD, la deuxième défenderesse fait valoir que l'argumentation du Service d'Inspection ne repose pas sur des constatations objectives mais que son analyse découle de demi-hypothèses et d'interprétations erronées. En ce qui concerne le traitement d'une catégorie particulière de données à caractère personnel, la deuxième défenderesse réitère son affirmation selon laquelle on peut mettre en doute l'existence d'un traitement de données biométriques et d'une catégorie particulière de données à caractère personnel dans le contexte du traitement pour la première défenderesse. La deuxième défenderesse ajoute que le Service d'Inspection a extrapolé ses conclusions à l'ensemble du fonctionnement et à toutes les activités de la deuxième défenderesse. La deuxième défenderesse souligne que ses activités sont réparties entre des services relatifs à des systèmes de stationnement et d'enregistrement du temps. Les chiffres de l'exercice 2021 indiquent que 74,29 % du chiffre d'affaires provient des systèmes de stationnement et 25,71 % de l'enregistrement du temps. L'enregistrement du temps en tant que tel va aussi au-delà des services Z. La part de la deuxième défenderesse dans le chiffre d'affaires total de Z n'était que de 8,50 % en 2021. La deuxième défenderesse dénonce la supposition du Service d'Inspection selon laquelle pour Z, la deuxième défenderesse aurait toujours recours aux lecteurs biométriques et mettrait donc en place pour d'autres clients une solution Z utilisant des lecteurs biométriques. Elle souligne que seuls 10,93 % du chiffre d'affaires sont spécifiquement générés par des projets liés à Z où des lecteurs biométriques sont également utilisés. La deuxième défenderesse se demande s'il existe des indices sérieux que ces projets utilisant des lecteurs biométriques impliquent le traitement d'une catégorie particulière de données. S'il y avait un traitement d'une catégorie particulière de données à caractère

personnel, ce que la deuxième défenderesse met en doute, cela ne doit pas nécessairement être le cas pour les autres clients utilisant l'application Z.

187. En ce qui concerne le caractère à grande échelle, la deuxième défenderesse dénonce le fait que le Service d'Inspection déduit le caractère à grande échelle entre autres du fait que Z est commercialisé dans 9 pays. La deuxième défenderesse souligne que toutes les solutions Z ne fonctionnent pas avec des lecteurs biométriques et que seules les solutions qui traitent effectivement des catégories particulières de données peuvent être prises en compte pour évaluer le caractère à grande échelle. La deuxième défenderesse conteste que, sur la base d'une enquête dans laquelle le Service d'Inspection conclut qu'il n'a aucune idée du nombre de personnes concernées ou de la quantité de données traitées mais constate que la durée et la permanence du traitement des données inhérentes à l'enregistrement du temps de travail constituent un élément supplémentaire pour apprécier le caractère à grande échelle du traitement, l'on puisse conclure au fait que le traitement présente un caractère de grande échelle.

188. La deuxième défenderesse se réfère enfin à la constatation du Service d'Inspection selon laquelle le critère du caractère principal se rapporte à l'activité principale du sous-traitant et pas à une activité connexe. Elle se pose la question de savoir si le traitement consistant à stocker la catégorie particulière dans le cadre de ses activités doit être considéré comme une activité principale. À cet égard, elle se réfère aux travaux préparatoires du RGPD qui précisent que par activités principales, on entend : "*les activités dans le cadre desquelles 50 % du chiffres d'affaires annuel résultant de la vente de données ou de recettes sont générés par l'utilisation de ces données*". Cela signifie *a contrario* que les activités de traitement de données qui ne génèrent pas plus de 50 % du chiffre d'affaires d'une entreprise sont considérées comme des activités connexes. La deuxième défenderesse attire l'attention sur le fait que le chiffre d'affaires généré par Z et impliquant des lecteurs biométriques ne représentait que 0,93 % de son chiffre d'affaires en 2021. Il n'est donc pas question d'une activité principale.

189. En ce qui concerne la prétendue obligation de désigner un délégué à la protection des données sur la base de l'article 37.1.b) du RGPD, la deuxième défenderesse souligne que les conditions cumulatives de caractère principal et à grande échelle ne sont pas revérifiées. En outre, la deuxième défenderesse attire l'attention sur le fait que ce n'est pas elle qui procède à un suivi régulier et systématique dans le cadre des traitements litigieux, si tant est qu'il en soit question.

II.14.3. Évaluation par la Chambre Contentieuse

190. En vertu de l'article 31.7 du RGPD, la désignation d'un délégué à la protection des données est obligatoire dans trois cas spécifiques :

a) lorsque le traitement est effectué par une autorité publique ou un organisme public ;

b) lorsque les activités de base du responsable du traitement ou du sous-traitant consistent en des opérations de traitement qui, du fait de leur nature, de leur portée et/ou de leurs finalités, exigent un suivi régulier et systématique à grande échelle des personnes concernées ; ou

c) lorsque les activités de base du responsable du traitement ou du sous-traitant consistent en un traitement à grande échelle de catégories particulières de données visées à l'article 9 et de données à caractère personnel relatives à des condamnations pénales et à des infractions.

191. Pour la désignation d'un délégué à la protection des données, l'article 37 du RGPD s'applique tant aux responsables du traitement qu'aux sous-traitants. En fonction de celui qui répond aux critères de désignation obligatoire, dans certains cas, seul le responsable du traitement ou seul le sous-traitant doit désigner un délégué à la protection des données, tandis que dans d'autres cas, les deux doivent le faire.

192. La question se pose de savoir si la deuxième défenderesse relève de l'un de ces 3 cas, de sorte que l'obligation de désigner un délégué à la protection des données lui incombe.

193. Vu que la deuxième défenderesse n'est pas une autorité publique, l'article 37.1.a) ne lui est pas applicable.

194. En ce qui concerne l'article 37.1.c) du RGPD, la Chambre Contentieuse rappelle que trois conditions cumulatives s'appliquent : (i) traitement de catégories particulières de données ou de données à caractère personnel relatives à des condamnations pénales et à des infractions, (ii) caractère à grande échelle et (iii) activité de base/principale.

195. Comme déjà établi ci-dessus, la Chambre Contentieuse rejoint la position de la deuxième défenderesse selon laquelle celle-ci ne traite pas de catégories particulières de données à caractère personnel au sens de l'article 9 du RGPD dans le cadre du contrat de sous-traitance conclu avec la première défenderesse. Le fait que la deuxième défenderesse offre la possibilité de traiter des données biométriques dans le cadre de Z n'implique pas automatiquement que la deuxième défenderesse traite des données biométriques pour tous ses clients. En outre, le traitement de données à caractère personnel biométriques n'implique pas automatiquement qu'il soit question d'un traitement d'une catégorie particulière de données à caractère personnel en vertu de l'article 9 du RGPD, vu qu'aucune identification ou vérification n'est prouvée. Par conséquent, il n'est pas démontré que la première condition soit remplie.

196. En ce qui concerne la condition relative au caractère à grande échelle, le RGPD ne prévoit aucune définition. En vertu du considérant 91, il s'agit des "*opérations de traitement à grande échelle qui visent à traiter un volume considérable de données à caractère personnel au*

niveau régional, national ou supranational, qui peuvent affecter un nombre important de personnes concernées et qui sont susceptibles d'engendrer un risque élevé [...]. La Chambre Contentieuse constate que le Service d'Inspection ne démontre pas que le traitement de catégories particulières de données à caractère personnel s'effectue à grande échelle. Le fait que Z soit distribué dans 9 pays européens ne prouve pas que des catégories particulières de données à caractère personnel au sens de l'article 9 du RGPD soient traitées à grande échelle. Enfin, en ce qui concerne le caractère à grande échelle, la Chambre Contentieuse constate que le chiffre d'affaires de la deuxième défenderesse généré par Z et impliquant des lecteurs biométriques ne représentait que 0,93 % du chiffre d'affaires de la deuxième défenderesse en 2021. La Chambre Contentieuse estime que c'est insuffisant pour parler d'une activité principale.

197. En outre, le Service d'Inspection fait observer que l'on peut également considérer sur la base de l'article 37.1.b) du RGPD que la deuxième défenderesse est tenue de désigner un délégué à la protection des données puisque l'enregistrement quotidien des heures d'arrivée et de départ des travailleurs sur le lieu de travail constitue un suivi régulier et systématique des personnes concernées. Dans ce cadre, la Chambre Contentieuse rejoint la position de la deuxième défenderesse selon laquelle l'éventuel suivi régulier et systématique est effectué par la première défenderesse dans le cadre de l'enregistrement du temps, et pas par la deuxième défenderesse. Elle ne propose en effet qu'un stockage pour des données (à caractère personnel) cryptées.

198. Au vu de ce qui précède, la Chambre Contentieuse constate dès lors qu'il n'y a **pas de violation de l'obligation, en vertu de l'article 37.1.b) et c) du RGPD,** de désigner un délégué à la protection des données.

III. Mesures correctrices

III.1. À l'égard de la première défenderesse

III.1.1. Violations constatées et mesures prises par la Chambre Contentieuse

III.1.1.1. Violations constatées

199. La Chambre Contentieuse a constaté les violations suivantes. Tout d'abord, la Chambre Contentieuse a constaté que la première défenderesse a traité illicitement des catégories particulières de données à caractère personnel dans le cadre du système d'enregistrement du temps et que dans ce contexte, elle a également violé les principes de limitation des finalités et de minimisation des données **(article 5.1.a) du RGPD, article 9.1, *j°* l'article 6.1 du RGPD, article 9.2 du RGPD 5.1.b) du RGPD, article 5.1.c) du RGPD).**

200. Ensuite, la Chambre Contentieuse a également jugé que la brochure d'accueil n'informait pas suffisamment les personnes concernées à propos du traitement litigieux.

Plus précisément, la brochure d'accueil ne respectait pas, de manière générale, l'obligation prévue à l'article 12.1 du RGPD, selon laquelle le responsable du traitement doit prendre des mesures appropriées pour que les informations visées à l'article 13 du RGPD soient reçues d'une façon concise, transparente, compréhensible et aisément accessible, en des termes clairs et simples et, en particulier, la Chambre Contentieuse constate que les délais de conservation(**(article 13.2.e) du RGPD**), les finalités et la base juridique ((**article 13.1.c) du RGPD**) ne figuraient pas (de manière adéquate) dans la brochure d'accueil. Étant donné que la première défenderesse invoque - certes illicitement - le consentement sur la base de l'article 6.1.a) et de l'article 9.2.a) du RGPD, il convenait également d'informer les personnes concernées qu'elles avaient le droit de retirer leur consentement **(article 3.2.c) du RGPD)**. En ce qui concerne la mention de la possibilité d'introduire une plainte auprès de l'Autorité de protection des données **(article 13.2.d) du RGPD**), la Chambre Contentieuse constate qu'elle ne figure pas non plus dans la brochure d'accueil.

201. En outre, la Chambre Contentieuse a constaté que la première défenderesse n'a pas fourni suffisamment d'informations lors de la deuxième demande d'accès, à savoir des informations sur la durée et les modalités de conservation des données et sur la sécurité des données, ce qui constitue une violation de l'obligation de la première défenderesse d'informer la personne concernée d'une façon compréhensible et aisément accessible, en des termes clairs et simples, comme le prévoit **l'article 15.1.d) *j°* l'article 12.1 du RGPD**.

202. De plus, la Chambre Contentieuse estime que plusieurs violations sont commises au niveau de l'obligation de documentation de la première défenderesse. En ce qui concerne le traitement de catégories particulières de données à caractère personnel dans le cadre de l'enregistrement du temps, la première défenderesse n'a pas effectué d'AIPD avant de commencer les traitements litigieux **(article 35 du RGPD**).

203. La première défenderesse a également omis de mentionner l'identité du délégué à la protection des données dans le registre des activités de traitement **(article 30.1.a) du RGPD)**. La première défenderesse a également violé l'article **30.1.b) et c) du RGPD** en ne mentionnant pas dans le registre des activités de traitement toutes les finalités et catégories de données à caractère personnel dans le cadre de l'enregistrement du temps, telles que reprises dans la version 2022 du règlement de travail. Enfin, la Chambre Contentieuse constate que la deuxième défenderesse, en sa qualité de sous-traitant dans le cadre du système biométrique d'enregistrement du temps, n'est pas mentionnée en tant que destinataire dans le registre des activités de traitement **(article 30.1.d) du RGPD)**.

204. Enfin, au vu des violations susmentionnées, la Chambre Contentieuse a constaté que la première défenderesse a commis une violation du principe de responsabilité au sens de l'article 5.2 du RGPD.

III.1.1.2. *Mesures prises par la Chambre Contentieuse*

205. Aux termes de l'article 100 de la 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 et des réprimandes ;
6° ordonner de se conformer aux demandes de la personne concernée d'exercer ses droits ;
7° ordonner que l'intéressé soit informé du problème de sécurité ;
8° ordonner le gel, la limitation ou l'interdiction temporaire ou définitive du traitement ;
9° ordonner une mise en conformité du traitement ;
10° ordonner la rectification, la restriction ou l'effacement des données et la notification de celles-ci aux récipiendaires des données ;
11° ordonner le retrait de l'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;
16° décider au cas par cas de publier ses décisions sur le site internet de l'Autorité de protection des données.

206. En ce qui concerne les violations constatées susmentionnées concernant l'obligation de documentation en vertu de **l'article 30.1.a), b), c) et d) du RGPD** et de **l'article 35 du RGPD**, la Chambre Contentieuse décide de formuler une réprimande sur la base de l'article 100, 5° de la LCA. L'importance de réaliser une AIPD en vertu de l'article 35 du RGPD ne peut pas être sous-estimée. L'obligation d'effectuer une AIPD vise à décrire le processus de traitement des données à caractère personnel afin d'identifier non seulement la nécessité et la proportionnalité du traitement, mais aussi les risques pour les droits et libertés des personnes concernées lors du traitement des données à caractère personnel. Le fait de ne pas effectuer d'AIPD constitue (donc) déjà en soi une violation du RGPD, tout en augmentant le risque de nouvelles violations du RGPD parce que les risques d'éventuelles (autres) violations du RGPD ne sont pas détectés à temps.

207. En ce qui concerne l'obligation de tenir un registre des activités de traitement en vertu de l'article 30 du RGPD, la Chambre Contentieuse souligne qu'afin de pouvoir appliquer efficacement les obligations contenues dans le RGPD, il est essentiel que le responsable du

traitement et les sous-traitants conservent un aperçu complet et précis des traitements de données à caractère personnel qu'ils effectuent. Ce registre des activités de traitement constitue dès lors en premier lieu un instrument pour aider le responsable du traitement ou le sous-traitant à respecter le RGPD pour les différents traitements de données qu'il réalise car le registre rend visibles les principales caractéristiques de ces traitements. La Chambre Contentieuse estime que ce registre des activités de traitement est un instrument essentiel dans le cadre du principe de **responsabilité** (déjà mentionné **article 5.2** et article 24 du RGPD) et que ce registre est à la base de toutes les obligations imposées par le RGPD au responsable du traitement et au sous-traitant. Il est dès lors de la plus haute importance que celui-ci soit complet et exact.

208. La Chambre Contentieuse estime qu'il y a suffisamment d'éléments pour formuler une réprimande pour les violations de l'**article 5.2, de l'article 30 et de l'article 35 du RGPD**, ce qui constitue une sanction légère et suffisante au vu des violations du RGPD constatées dans ce dossier. Pour déterminer la sanction, la Chambre Contentieuse tient compte du fait que la première défenderesse a déjà pris plusieurs mesures pour se conformer à ses obligations telles que prescrites par le RGPD et en apporte la preuve.

209. En ce qui concerne la violation due à la suite incomplète donnée à la deuxième demande d'accès (**à l'article 15.1.d)*j*° l' article 12.1 du RGPD**), la Chambre Contentieuse met en garde la première défenderesse pour l'avenir, sur la base de l'article 100, 5° de la LCA, d'une part, que le fait que les données à caractère personnel de la personne concernée ne sont plus traitées par le responsable du traitement ne signifie pas que le droit d'accès ne doit plus être exécuté et d'autre part, que si les informations demandées ne figurent pas dans l'énumération reprise à l'article 15.1 du RGPD, cela ne signifie pas qu'aucune réponse ne doit être formulée à une demande d'accès, étant donné que l'obligation de fournir des informations de façon concise, transparente, compréhensible et facilement accessible porte également sur l'obligation d'information visée à l'article 13 du RGPD. Le fait que ces informations soient demandées dans le cadre d'une demande d'accès ne signifie pas qu'aucune suite ne doive être donnée à cette demande d'informations. La Chambre Contentieuse estime qu'un avertissement suffit, vu qu'il n'est pas exact que la première défenderesse a mis le plaignant dans l'impossibilité totale d'exercer son droit d'accès. Au contraire, la première défenderesse avait déjà répondu à la première demande d'accès du plaignant, réponse qui a été partiellement reprise dans sa réponse à la deuxième demande d'accès du plaignant.

210. En ce qui concerne les violations de l'**article 5.1.a) du RGPD, de l'article 6.1 RGPD, de l'article 9.1 et 9.2 du RGPD, de l'article 5.1.b) du RGPD, de l'article 5.1.c) du RGPD** relatives aux principes de licéité, de limitation des finalités et de minimisation des données et la violation de l'**article 13.1.c), de l'article 13.2.c), 13.2.d) et 13.2.e) du RGPD** relative à

l'obligation d'information, la Chambre Contentieuse décide de procéder à l'imposition d'une amende administrative en vertu des pouvoirs que lui confèrent l'article 83 du RGPD et l'article 100, § 1er, 13° de LCA.

III.1.1.3. Calcul de l'amende

211. L'EDPB a adopté le 24 mai 2023 les Lignes directrices 04/2022 sur le calcul des amendes administratives au titre du RGPD[32] (ci-après : les Lignes directrices). Les Lignes directrices sont immédiatement applicables car elles ne prévoient pas de droit transitoire pour les procédures qui étaient déjà en cours au moment de l'adoption des Lignes directrices. La Chambre Contentieuse va dès lors appliquer ces Lignes directrices à la présente affaire.

212. Les Lignes directrices décrivent une méthodologie pour déterminer le montant de l'amende comme suit :

Étape 1 : recenser les traitements et les violations qui doivent être évalués ;

Étape 2 : fixer le montant de départ pour le calcul de l'amende pour les violations constatées (montant de départ) ;

Étape 3 : apprécier les circonstances aggravantes et atténuantes qui nécessitent, le cas échéant, l'adaptation du montant fixé à l'étape 2 ;

Étape 4 : déterminer les montants maximaux applicables pour les violations et si les majorations éventuelles de l'étape précédente ne dépassent pas ces montants ;

Étape 5 : déterminer si le montant final de l'amende calculée est bien effectif, proportionné et dissuasif et adapter ce montant à ces critères, si nécessaire.

213. La Chambre Contentieuse déterminera le montant de l'amende administrative à l'aide de cette méthodologie.

III.1.1.4. Étape 1 : recenser les traitements et les violations qui doivent être évalués ;

214. Afin de déterminer le montant de départ de l'amende, il convient tout d'abord, comme décrit dans les Lignes directrices, d'examiner s'il existe un ou plusieurs comportements susceptibles d'être sanctionnés. La Chambre Contentieuse a constaté que la première défenderesse a traité illicitement des catégories particulières de données à caractère personnel dans le cadre du système d'enregistrement du temps et que dans ce contexte, elle a également violé les principes de limitation des finalités et de minimisation des données

[32] EDPB - Lignes directrices 04/2022 sur le calcul des amendes administratives au titre du RGPD (V2.1, 24 mai 2023), consultable via le lien suivant : https://www.edpb.europa.eu/system/files/2024-01/edpb_guidelines_042022_calculationofadministrativefines_fr_0.pdf.

(article 5.1.a) du RGPD, article 6.1 du RGPD, article 9.2 du RGPD, article 5.1.b) du RGPD, article 5.1.c) du RGPD).

215. Ensuite, la Chambre Contentieuse a également jugé que la brochure d'accueil n'informait pas suffisamment les personnes concernées à propos du traitement litigieux. Plus précisément, la brochure d'accueil ne contenait pas suffisamment d'informations entre autres sur les délais de conservation (**article 13.2.e) du RGPD**), les finalités et la base juridique (**article 13.1.c)** du RGPD). La Chambre Contentieuse estime que ces éléments n'ont pas été (suffisamment) repris dans la brochure d'accueil. Étant donné que la première défenderesse invoque - certes illicitement - le consentement sur la base de l'article 6.1.a) et de l'article 9.2.a) du RGPD, il convenait également d'informer les personnes concernées qu'elles avaient le droit de retirer leur consentement **(article 13.2.c) du RGPD)**. En ce qui concerne la mention de la possibilité d'introduire une plainte auprès de l'APD **(article 13.2.d) du RGPD)**, la Chambre Contentieuse constate qu'elle ne figure pas non plus dans la brochure d'accueil.

216. La Chambre Contentieuse estime qu'il s'agit en l'espèce d'un seul comportement sanctionnable. Dans ce contexte, la Chambre Contentieuse renvoie aux Lignes directrices qui précisent que lorsqu'il est question d'évaluer "[une] même opération de traitement ou [des] opérations de traitement liées", il convient de garder à l'esprit que toutes les obligations nécessaires sur le plan juridique pour que les opérations de traitement soient réalisées dans le respect des lois peuvent être prises en considération par l'autorité de contrôle dans le cadre de son appréciation des violations, y compris [...] les obligations en matière de transparence (par ex. l'article 13 du RGPD). Ce point est également mis en avant par les termes "dans le cadre de la même opération de traitement ou d'opérations de traitement liées", qui indiquent que le champ d'application de cette disposition englobe toute violation liée aux mêmes opérations de traitement ou à des opérations de traitement liées et susceptibles d'avoir une incidence sur celles-ci.[33] La Chambre Contentieuse constate que les violations établies ci-dessus concernant les principes de licéité, de limitation des finalités, de minimisation des données, d'obligation d'information et de responsabilité sont liées à la même activité de traitement, à savoir le système d'enregistrement du temps de travail par empreintes digitales. Par conséquent, la Chambre Contentieuse estime que les circonstances constituent un seul et même comportement qui donnera lieu à l'imposition d'une seule amende pour les violations résultant du comportement en question.

III.1.1.5. Étape 2 : fixer le montant de départ

[33] EDPB - Lignes directrices 04/2022 sur le calcul des amendes administratives au titre du RGPD (V2.1, 24 mai 2023), p. 13, https://edpb.europa.eu/system/files/2024-01/edpb_guidelines_042022_calculationofadministrativefines_fr_0.pdf.

217. Comme décrit dans les Lignes directrices, il convient ensuite de fixer le montant de départ de l'amende. Ce montant de départ constitue le point de départ du calcul ultérieur dans les étapes suivantes, où tous les faits et circonstances pertinents sont pris en considération. Les Lignes directrices indiquent que le montant de départ est déterminé au moyen de trois éléments : i) la qualification des violations au titre de l'article 83, paragraphes 4 à 6 du RGPD (étape 2.1) ; ii) la gravité de la violation (étape 2.2) et iii) le chiffre d'affaires de l'entreprise (étape 2.3).

III.1.1.5.1. *Étape 2.1 : Qualification des violations au titre de l'article 83, paragraphes 4 à 6 du RGPD*

218. Comme mentionné dans les Lignes directrices, presque toutes les obligations du responsable du traitement sont qualifiées dans les dispositions de l'article 83, paragraphes 4 à 6 du RGPD. Le RGPD établit une distinction entre deux types de violations. D'une part les violations sanctionnables au titre de l'article 83.4 du RGPD et passibles d'une amende maximale de 10 millions d'euros (ou dans le cas d'une entreprise, de 2 % du chiffre d'affaires annuel, le montant le plus élevé étant retenu), d'autre part les violations sanctionnables au titre de l'article 83, paragraphes 5 et 6 du RGPD et passibles d'une amende maximale de 20 millions d'euros (ou dans le cas d'une entreprise, de 4 % du chiffre d'affaires annuel, le montant le plus élevé étant retenu). Par cette distinction, le législateur a donné une première indication *in abstracto* de la gravité de la violation : plus la violation est grave, plus l'amende est élevée.

219. Pour les violations en question de **l'article 5.1.a) du RGPD, de l'article 6.1 du RGPD, de l'article 9.1 et 9.2 du RGPD, de l'article 5.1.b) du RGPD, de l'article 5.1.c) du RGPD, de l'article 13.1.c), 13.2.c), d) et e) du RGPD *j°* l'article 12.1 du RGPD,** une amende administrative de maximum 20 millions d'euros peut être infligée, ou dans le cas d'une entreprise, de 4 % du chiffres d'affaires annuel mondial, le montant le plus élevé étant retenu (article 83.5 du RGPD). Il découle de cette qualification que les violations de ces dispositions sont considérées comme graves par le législateur.

III.1.1.5.2. *Gravité des violations dans la présente affaire*

220. Afin de déterminer la gravité de la violation, les Lignes directrices prévoient qu'il convient de tenir compte de la nature, de la gravité et de la durée de la violation, ainsi que du caractère délibéré ou négligent de la violation et des catégories de données à caractère personnel concernées.

221. **Nature de la violation -** Les Lignes directrices prévoient que l'autorité de contrôle peut se pencher sur l'intérêt que la disposition enfreinte œuvre à protéger et l'importance de cette disposition dans le cadre de la protection des données. En ce qui concerne la licéité, le RGPD dispose qu'il existe six bases pour un traitement licite de données à caractère personnel.

Lorsqu'il entreprend des activités qui impliquent le traitement de données à caractère personnel, le responsable du traitement doit toujours prendre le temps d'examiner quelle serait la base juridique appropriée pour le traitement envisagé[34]. La base juridique applicable influence également les droits applicables des personnes concernées ou les obligations d'information applicables. Les violations de ces principes fondamentaux constituent dès lors des manquements graves, passibles des amendes administratives les plus élevées prévues par le RGPD. Par conséquent, la Chambre Contentieuse conclut que la licéité occupe une place centrale dans le cadre de la protection des données et justifie donc l'imposition d'une amende.

222. **Nature, gravité et durée de la violation (article 83.2.a) du RGPD)** - En ce qui concerne la **gravité** de la violation, la Chambre Contentieuse observe que le principe de licéité (article 5.1.a) et article 6 du RGPD), conjointement avec les principes de limitation des finalités (article 5.1.b) du RGPD) et de minimisation des données (article 5.1.c) du RGPD) sont des principes fondamentaux de la protection garantie par le RGPD. En outre, le responsable du traitement devrait fournir à la personne concernée les informations nécessaires pour garantir un traitement équitable et transparent, compte tenu des circonstances particulières et du contexte dans lesquels les données à caractère personnel sont traitées.

223. En ce qui concerne la nature du traitement, la Chambre Contentieuse observe qu'une base juridique valable et des informations transparentes font partie des éléments clés du droit fondamental à la protection des données. Les violations de ces principes fondamentaux constituent dès lors des manquements graves, passibles des amendes administratives les plus élevées prévues par le RGPD.

224. Dans sa réaction au formulaire de sanction, la première défenderesse ne conteste pas la gravité de la violation, mais souligne que cette gravité doit être appréciée à la lumière de l'ensemble des circonstances ci-dessous, propres à cette affaire. Elle souligne que la nature du traitement ne présentait pas un risque élevé car le système mis en place par la deuxième défenderesse permettait uniquement d'associer un code aux données sensibles, l'empreinte digitale numérique restant dans le hardware. Par conséquent, le traitement des données sensibles permettait seulement de créer un code qui était ensuite associé au dossier individuel du travailleur, où seules les heures prestées étaient enregistrées. Les données sensibles ne sont ni reproduites, ni communiquées, ni analysées. Seules les heures de pointage sont relevées et associées à un code, l'empreinte digitale reste dans le hardware de la deuxième défenderesse qui, comme le relève la première défenderesse, ne semble pas être critiqué par la Chambre Contentieuse. La Chambre Contentieuse tient compte de ces circonstances à l'étape 3 lors de l'évaluation d'éventuelles circonstances

[34] EDPB - Lignes directrices 5/2020 sur le consentement au sens du Règlement 2016/679 (5 mai 2020), p. 5 https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_fr.pdf.

aggravantes ou atténuantes, comme le prescrivent les Lignes directrices.[35] Conformément aux Lignes directrices, chaque critère de l'article 83.2 du RGPD ne peut être pris en compte qu'une seule fois.

225. En ce qui concerne la **finalité** du traitement, la Chambre Contentieuse constate que le traitement avait pour finalité d'enregistrer le temps de travail des travailleurs et de calculer et payer les salaires sur cette base. Comme indiqué également, aucun paiement ne pouvait être effectué si aucun pointage n'était enregistré, ce qui permettait de prendre des mesures ayant des conséquences négatives. Conformément aux Lignes directrices, la Chambre Contentieuse accorde davantage de poids à ce facteur compte tenu de la relation entre les personnes concernées en tant que travailleurs et la première défenderesse en tant qu'employeur.[36]

226. Dans sa réaction au formulaire de sanction, la première défenderesse indique qu'elle est active dans la production de produits d'emballage en métal léger (canettes en aluminium). À ce titre, elle ne traite que des données relatives aux heures de travail, obtenues par pointage biométrique d'entrée et de sortie. Les données sensibles restent en effet sécurisées et stockées dans le système de la deuxième défenderesse. La périphérie de l'activité principale est dès lors limitée au calcul des salaires, basé sur l'enregistrement du temps de travail.

227. La Chambre Contentieuse observe toutefois que la finalité avancée du traitement litigieux aurait également pu être atteinte sans le traitement des données à caractère personnel biométriques en question. Le traitement des données à caractère personnel ne constitue pas une activité principale de la première défenderesse, mais constitue néanmoins une importante activité connexe dans l'accomplissement de sa tâche principale. La Chambre Contentieuse accorde un poids important à ce facteur.

228. En ce qui concerne la **gravité** de la violation, la Chambre Contentieuse prend en considération que le traitement illicite dans le cadre de l'enregistrement du temps en question s'appliquait à tous les travailleurs. Il en va de même pour l'obligation d'information des travailleurs, au moins jusqu'à l'adoption du règlement de travail 2022. Ensuite, pour évaluer la gravité de la violation, la Chambre Contentieuse prend certes en compte les violations commises mentionnées ci-avant. Toutefois, il n'est pas établi que la première défenderesse ait totalement manqué à ses obligations en vertu du RGPD. La première défenderesse a invoqué, de manière illicite, le consentement comme base juridique pour le traitement litigieux. Bien que la Chambre Contentieuse ait constaté plusieurs violations de l'obligation d'information à propos du traitement litigieux, on ne peut pas dire que la

[35] EDPB - Lignes directrices 04/2022 sur le calcul des amendes administratives au titre du RGPD (V2.1, 24 mai 2023), p. 29.

[36] EDPB - Lignes directrices 5/2020 sur le consentement au sens du Règlement 2016/679 (5 mai 2020), p. 20 https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_fr.pdf.

première défenderesse ait totalement omis d'informer ses travailleurs sur le traitement en question. En outre, il n'apparaît pas non plus que les travailleurs aient subi un préjudice substantiel suite au traitement litigieux et au manquement à l'obligation d'information. La Chambre Contentieuse accorde un poids léger à ce facteur.

229. En ce qui concerne **la durée** , il a été constaté que le système d'enregistrement du temps litigieux a été introduit le 16 mars 2020 et interrompu suite au rapport d'inspection fin 2022, ce qui constitue une période relativement courte. En ce qui concerne la durée de la violation, la première défenderesse indique dans sa réponse au formulaire de sanction qu'elle est une entreprise relativement jeune qui a commis une erreur dans le système d'enregistrement des heures de travail. Elle ajoute qu'elle a immédiatement mis fin au système d'enregistrement du temps. La Chambre Contentieuse accorde un poids léger à ce facteur.

230. En ce qui concerne la portée du traitement, la première défenderesse fait valoir que les données sensibles en question, à savoir les empreintes digitales, restent verrouillées et sécurisées dans le système hardware de la deuxième défenderesse. La portée du traitement est donc très locale et montre que le risque est très faible, voire inexistant, vu que les données sensibles restent dans le système de la deuxième défenderesse, qui est sécurisé et verrouillé. La première défenderesse elle-même ne dispose pas de l'empreinte digitale, mais seulement du code crypté lié à l'empreinte digitale et aux données d'enregistrement du temps de travail. La première défenderesse relève que ce code lui-même est généré par l'équipement de la deuxième défenderesse et que la clé de cryptage n'est pas connue de la première défenderesse, si elle souhaitait obtenir l'empreinte digitale en tant que telle. L'ampleur du traitement local ne permettait pas d'exclure toute association entre le code et les empreintes digitales stockées dans le hardware de la deuxième défenderesse, de sorte que le risque de diffusion était très faible. La Chambre Contentieuse tient compte de ces circonstances à l'étape 3 lors de l'évaluation d'éventuelles circonstances aggravantes ou atténuantes, comme le prescrivent les Lignes directrices.[37] Conformément aux Lignes directrices, chaque critère de l'article 83.2 du RGPD ne peut être pris en compte qu'une seule fois.

231. **Caractère négligent ou délibéré de la violation (article 83.2.b) du RGPD) —** La Chambre Contentieuse rappelle qu'en général, l' "intention" comprend à la fois la connaissance et la volonté en rapport avec les caractéristiques d'une infraction, tandis que les termes "non délibérément" signifient qu'il n'y a pas eu d'intention de causer la violation, bien que le responsable du traitement ou le sous-traitant ait violé l'obligation de diligence prescrite par la législation.[38] En d'autres termes, deux éléments cumulatifs sont nécessaires pour qu'une

[37] EDPB - Lignes directrices 04/2022 sur le calcul des amendes administratives au titre du RGPD (V2.1, 24 mai 2023), p. 29.

[38] Groupe de travail "Article 29" sur la protection des données - Lignes directrices sur l'application et la fixation des amendes administratives.

aux fins du règlement (UE) 2016/679 (WP 253, 3 octobre 2017), p. 12.

violation soit considérée comme intentionnelle, à savoir la connaissance de la violation et la volonté en relation avec cet acte.[39]

232. En ce qui concerne la composante intentionnelle, la Chambre Contentieuse rappelle également que la Cour de justice a fixé un seuil élevé pour qu'un acte puisse être considéré comme intentionnel. La Cour de justice a ainsi estimé dans des affaires pénales qu'il est question d'une "négligence grave" plutôt que d'une "intention" lorsque "la personne responsable viole, d'une manière caractérisée, l'obligation de diligence qu'elle aurait dû et aurait pu respecter compte tenu de ses qualités, de ses connaissances, de ses aptitudes et de sa situation individuelle."[40] Même si on peut attendre d'une entreprise dont le traitement de données à caractère personnel n'est pas l'activité principale qu'elle prenne suffisamment de mesures pour protéger les données à caractère personnel et qu'elle reconnaisse pleinement ses obligations à cet égard, une telle violation qualifiée ne démontre pas nécessairement qu'il s'agit d'une violation délibérée.[41]

233. En d'autres termes, cela signifie qu'un responsable du traitement peut également être sanctionné par une amende administrative en vertu de l'article 83 du RGPD pour un comportement relevant du champ d'application du RGPD, lorsque ce responsable du traitement ne pouvait ignorer que son comportement constituait une violation, indépendamment du fait qu'il était conscient ou non qu'il violait les dispositions du RGPD.[42] Selon la Chambre Contentieuse, il n'y a pas d'intention - manifeste - dans le chef de la deuxième défenderesse de violer délibérément le RGPD dans le cadre de l'introduction du système d'enregistrement du temps au moyen de données biométriques, ni dans le contexte du manquement à l'obligation d'information. La Chambre Contentieuse estime par contre qu'il y a eu négligence lors de la commission des violations. Les violations constatées sont dues à une erreur d'appréciation de la première défenderesse. Elle a pris la prévention de la fraude comme point de départ dans le cadre de l'enregistrement du temps, ce qui constitue une finalité légitime, mais à cet égard, la partie défenderesse aurait également dû évaluer le respect du RGPD. On peut attendre d'une professionnelle telle que la première défenderesse, compte tenu notamment de la nature particulière des données à caractère

---

[39] Voir également EDPB - Binding Decision 1/2023 on the dispute submitted by the Irish SA on data transfers by Meta Platforms Ireland

Ltd (Facebook), point 103, disponible via le lien suivant : https://www.edpb.europa.eu/our-work-tools/our-documents/binding-decision-board-art-65/binding-decision-12023-dispute-submitted_fr.

[40] CJUE, 3 juin 2008, C-308/06, Intertanko e.a. (ECLI:EU:C:2008:312), point 77.

[41] Voir également EDPB – Binding Decision 2/2022 on the dispute arisen on the draft decision of the Irish Supervisory Authority regarding Meta Platforms Ireland Limited (Instagram) under Article 65(1)(a) GDPR, 28 juillet 2022, point 204.

[42] CJUE, 5 décembre 2023, C-807/21, *Deutsche Wohnen SE c. Staatsanwaltschaft Berlin* (ECLI:EU:C:2023:950), point 76.

Voir également CJUE, 18 juin 2013, C-681/11, *Schenker & Co. e.a.* (ECLI:EU:C:2013:404), point 37 ; CJUE, 25 mars 2021, *Lundbeck c. Commission*, C-591/16 P (ECLI:EU:C:2021:243), point 156 ; et CJUE 25 mars 2021, C-601/16 P, *Arrow Group en Arrow Generics c. Commission* (ECLI:EU:C:2021:244), point 97.

personnel, qu'elle soit pleinement consciente des normes qui lui sont applicables et qu'elle s'y conforme.

234. Dans sa réponse au formulaire de sanction, la première défenderesse rejoint la position de la Chambre Contentieuse et rappelle qu'elle a souhaité introduire un système de prévention de la fraude relative aux heures de travail, ce problème étant effectivement présent et ayant été démontré dans le cadre de la présente procédure. La première défenderesse reconnaît qu'elle aurait dû utiliser un autre système pour l'enregistrement du temps de travail.

235. La Chambre Contentieuse reconnaît la nécessité pour la première défenderesse de faire face et/ou de prévenir la fraude éventuelle et attribue un poids moyen à ce facteur.

236. **Catégories de données à caractère personnel concernées par la violation (article 83.2.g) du RGPD)** - Les Lignes directrices soulignent que le RGPD identifie clairement les types de données qui nécessitent une protection particulière et pour lesquelles les amendes devraient donc être plus sévères. Il s'agit en tout cas ici des types de données visées aux articles 9 et 10 du RGPD. En général, plus ces catégories de données sont nombreuses ou plus les données sont sensibles, plus l'autorité de contrôle peut attribuer de poids à ce facteur.[43] La Chambre Contentieuse a qualifié les données à caractère personnel traitées par la première défenderesse de particulières au sens de l'article 9 du RGPD. Les violations constatées concernant la licéité et l'obligation d'information concernent dès lors également les données à caractère personnel au sens de l'article 9 du RGPD, raison pour laquelle la Chambre Contentieuse attribue plus de poids à ce facteur.

III.1.1.5.3. *Chiffre d'affaires de la société*

237. La Chambre Contentieuse précise à cet égard qu'au moment de l'envoi du formulaire de sanction en date du 4 juin 2024, elle ne disposait pas encore des chiffres d'affaires de l'année 2023 et a donc dû prendre en considération les chiffres d'affaires de l'année 2022. Après l'envoi du formulaire de sanction, les comptes annuels de l'exercice 2023 ont été publiés sur le site Internet de la Banque nationale de Belgique, où un chiffre d'affaires de 85.444.466 euros a été inscrit.

i. Conclusion relative au montant de départ

a. Montant de départ théorique (sur la base de la gravité de la violation)

238. En vertu de l'article 83.5 du RGPD, l'amende s'élève au maximum à 20 millions d'euros ou, dans le cas d'une entreprise, jusqu'à 4 % du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu, ce qui n'est pas le cas en l'occurrence. Le montant maximum légal s'élève donc à 20 millions d'euros.

---

[43] EDPB - Lignes directrices 04/2022 sur le calcul des amendes administratives au titre du RGPD (V2.1, 24 mai 2023), p. 22, https://edpb.europa.eu/system/files/2024-01/edpb_guidelines_042022_calculationofadministrativefines_fr_0.pdf.

239. Sur la base de l'évaluation des critères exposés ci-dessus, la Chambre Contentieuse doit déterminer si la violation est jugée d'une gravité faible, moyenne ou élevée. Ces catégories n'enlèvent rien à la question de savoir si une amende peut être infligée ou non.[44]

240. Cette évaluation n'est pas un calcul mathématique dans lequel les facteurs précités sont considérés séparément, mais plutôt une évaluation approfondie des circonstances concrètes de l'espèce, tous les facteurs précités étant mutuellement liés. C'est pourquoi lors de l'évaluation de la gravité de la violation, il faut considérer la violation dans son ensemble.[45]

▪ Lors du calcul de l'amende administrative à infliger pour les violations de gravité faible, l'autorité de contrôle fixe un montant de départ pour le calcul ultérieur compris entre 0 et 10 % du maximum légal applicable.

▪ Lors du calcul de l'amende administrative à infliger pour les violations de gravité moyenne, l'autorité de contrôle fixe un montant de départ pour le calcul ultérieur compris entre 10 et 20 % du maximum légal applicable.

▪ Pour les violations de gravité élevée, lors du calcul de l'amende administrative, l'autorité de contrôle fixe un montant de départ pour le calcul ultérieur compris entre 20 et 100 % du montant maximal légal applicable.[46]

241. En règle générale, plus la violation est grave dans la catégorie concernée, plus le montant de départ est susceptible d'être élevé.[47]

242. Dans sa réponse au formulaire de sanction, la première défenderesse indique que, compte tenu des critères ci-dessus, le degré de gravité de la violation pourrait être considéré comme faible. Elle se réfère à cet égard aux éléments examinés ci-avant tels que la nature du traitement, la portée du traitement, la finalité du traitement, l'ampleur du préjudice et la durée de la violation.

243. La Chambre Contentieuse a constaté qu'il était question d'une violation de l'article 5.1.a), b) et c) du RGPD, de l'article 9.1 *j°* les articles 6.1 et 9.2 du RGPD, d'une part, et d'une violation de l'article 13.1.c) et 13.2.c), d) et e) du RGPD *j°* l'article 12.1, d'autre part, qui sont repris dans les violations de l'article 83.5 du RGPD. Ensuite, la Chambre Contentieuse a réalisé une analyse de la nature de la violation, de sa finalité, de l'ampleur et de la durée du traitement, ainsi que des catégories des données à caractère personnel traitées et du caractère négligent de la violation.[48]

---

[44]EDPB, Lignes directrices 04/2022 sur le calcul des amendes administratives au titre du RGPD V2.1, 24 mai 2023), p. 23, https://edpb.europa.eu/system/files/2024-01/edpb_guidelines_042022_calculationofadministrativefines_fr_0.pdf.

[45]EDPB - Lignes directrices 04/2022 sur le calcul des amendes administratives au titre du RGPD V2.1, 24 mai 2023), p. 23, https://edpb.europa.eu/system/files/2024-01/edpb_guidelines_042022_calculationofadministrativefines_fr_0.pdf.

[46] EDPB - Lignes directrices 04/2022 sur le calcul des amendes administratives au titre du RGPD (V2.1, 24 mai 2023), p. 23

[47] EDPB - Lignes directrices 04/2022 sur le calcul des amendes administratives au titre du RGPD (V2.1, 24 mai 2023), p. 23

[48] Voir les points 95 à 102 inclus de la présente décision.

244. Se basant sur les évaluations précédentes des circonstances précitées, la Chambre Contentieuse estime que le comportement relevant de l'article 83.5 du RGPD est en soi de gravité moyenne. À cet égard, la Chambre Contentieuse tient compte, d'une part, notamment de la nature sensible des données personnelles biométriques et de leur caractère, de la capacité professionnelle de la première défenderesse en tant qu'employeur vis-à-vis du plaignant, et de la portée large, étant donné que le système d'enregistrement des heures s'applique à tous les travailleurs.

245. D'autre part, la Chambre Contentieuse tient également compte de la durée relativement limitée de la violation, du caractère involontaire de la négligence dans le chef de la première défenderesse et du fait qu'elle a informé les personnes concernées, bien que de manière incomplète, du traitement litigieux.

246. Dès lors, le montant de départ pour la suite du calcul doit être fixé à un montant entre 10 % et 20 % du maximum légal applicable. La Chambre Contentieuse décide de fixer un montant de départ *théorique* de 2 millions d'euros par violation, soit 10 % du montant maximum légal applicable de 20 millions d'euros (art. 83.5 du RGPD).

b. Adaptation du montant de départ sur la base de la taille de l'entreprise

247. Ensuite, la Chambre Contentieuse doit vérifier si le montant de départ doit être adapté en fonction de la taille de l'entreprise. Cette adaptation n'est valable que pour les entreprises auxquelles s'applique la limite légale statique, à savoir lorsque l'entreprise a réalisé un chiffre d'affaires de moins de 500 millions d'euros au cours de l'exercice précédent. Étant donné que c'est le cas en l'espèce, l'amende doit être adaptée en fonction de la limite légale statique.

248. La Chambre Contentieuse a déjà expliqué que le comportement constaté ci-dessus relevait de l'article 83.5 du RGPD et était d'une gravité moyenne. Pour les violations mentionnées à l'article 83.5 du RGPD, de gravité moyenne, appliquées à une entreprise ayant un chiffre d'affaires entre 50 millions d'euros et 100 millions d'euros, l'amende s'élève à 8 à 20 % du montant de départ, l'amende ne pouvant pas être inférieure à 160.000 euros ni être supérieure à 800.000 euros.[49]

249. Compte tenu des montants minimaux et maximaux fixés dans les Lignes directrices par niveau, d'une part, et du chiffre d'affaires pertinent du responsable du traitement, d'autre part, la Chambre Contentieuse décide de réduire le montant de départ final de chacune des violations constatées (relevant de l'article 83.5 du RGPD avec une gravité moyenne) pour atteindre un montant de départ *adapté* de 160.000 euros, soit 8 % du montant de départ théorique de 2 millions d'euros.

[49] EDPB - Lignes directrices 04/2022 sur le calcul des amendes administratives au titre du RGPD (V2.1, 24 mai 2023), p. 52.

III.1.1.6. Étape 3 : évaluation des circonstances aggravantes et atténuantes

i) Évaluation de l'application des éventuelles circonstances aggravantes ou atténuantes

250. Comme mentionné dans les lignes directrices, il faut ensuite évaluer si, dans les circonstances en l'espèce, il y a lieu de fixer une amende plus ou moins élevée que le montant de départ défini à cet égard. Les circonstances à prendre en compte sont énoncées à l'article 83.2, *ab initio* et aux points a) à k) inclus du RGPD. Chacune des circonstances mentionnées dans cette disposition ne peut être évaluée qu'une fois [50]. Dans l'étape précédente, il a déjà été tenu compte de la nature, de l'importance et de la durée de la violation[51], de la nature intentionnelle ou négligente de la violation[52] et des catégories de données à caractère personnel[53]. Il reste donc encore les parties c) à f) inclus et h) à k) inclus.

251. **Mesures prises pour atténuer le dommage subi par les personnes concernées (article 83.2.c) du RGPD) –** Comme indiqué dans les Lignes directrices WP 253 du Groupe 29[54], les responsables du traitement et les sous-traitants sont déjà tenus "de mettre en œuvre les mesures techniques et organisationnelles afin de garantir un niveau de sécurité adapté au risque, d'effectuer des analyses d'impact relatives à la protection des données et d'atténuer les risques pour les droits et les libertés des personnes résultant du traitement des données à caractère personnel". Dans le cas où une violation a lieu, le responsable du traitement ou le sous-traitant doit donc faire "tout ce qui est en son pouvoir" pour réduire les conséquences de la violation pour la (les) personne(s) concernée(s). En l'espèce, la première défenderesse aurait dû s'abstenir de traiter les données biométriques de ses travailleurs. En le faisant quand même, la première défenderesse a violé l'essence de cette obligation. Étant donné que les travailleurs de la première défenderesse ont été insuffisamment informés du traitement et qu'il n'est pas établi qu'ils ont donné (librement) leur consentement explicite, la première défenderesse a commis, en réalisant ce traitement, une violation de la protection des données à caractère personnel de ses travailleurs.

252. **La mesure dans laquelle le responsable du traitement ou le sous-traitant est responsable au vu des mesures techniques et organisationnelles qu'il a mises en œuvre conformément aux articles 25 et 32 du RGPD (article 83.2.c) du RGPD)** –Dans la section II.8, la Chambre Contentieuse a constaté que la première défenderesse a pris différentes mesures organisationnelles pour sécuriser les données à caractère personnel en question. En outre, la première défenderesse a eu recours à la deuxième défenderesse en ce qui concerne la

[50] EDPB - Lignes directrices 04/2022 sur le calcul des amendes administratives au titre du RGPD (V2.1, 24 mai 2023), p. 23.

[51] Voir les points 95-98 de la présente décision.

[52] Voir le point 99-101 de la présente décision.

[53] Voir le point 102 de la présente décision.

[54] Groupe de travail "Article 29" sur la protection des données – Lignes directrices *sur l'application et la fixation des amendes administratives aux fins du règlement (UE) 2016/679* (3 octobre 2017).

sécurisation technique des données à caractère personnel. La Chambre Contentieuse a constaté aux points II.7 et II.8 qu'il n'y avait pas de violation de l'article 32 du RGPD. Par conséquent, la Chambre Contentieuse tient compte du fait que la première défenderesse a bien manifesté l'intention de protéger adéquatement les données à caractère personnel particulières traitées et a également conclu à cette fin un contrat de sous-traitance avec la deuxième défenderesse. À cet égard, la Chambre Contentieuse tient particulièrement compte du fait que les empreintes digitales en soi n'ont pas quitté l'environnement sécurisé de la deuxième défenderesse et que la première défenderesse disposait uniquement d'un code pouvant être associé à l'enregistrement du temps, et ce comme circonstance atténuante.

253. **Violation pertinente commise précédemment par le responsable du traitement ou le sous-traitant (article 83.2.e) du RGPD) –** La Chambre Contentieuse tient compte du fait qu'à ce jour, elle n'a été saisie d'aucune autre procédure à l'encontre de la première défenderesse. Conformément aux Lignes directrices, ce facteur doit donc être considéré comme étant neutre.[55]

254. **La manière dont l'autorité de contrôle a eu connaissance de la violation (article 83.2.h) –** Étant donné que la Chambre Contentieuse a eu connaissance de la violation suite à une plainte, cet élément est réputé neutre conformément aux Lignes directrices.[56]

255. **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 (article 83.2.f) du RGPD) —** La Chambre Contentieuse fait remarquer que la deuxième défenderesse s'est montrée coopérante à son égard. Conformément aux Lignes directrices, la Chambre Contentieuse considère l'obligation ordinaire de coopération comme étant neutre, vu l'obligation générale de coopération inscrite à l'article 31 du RGPD.

256. Dans sa réponse au formulaire de sanction, la première défenderesse souligne que non seulement elle a pleinement coopéré, mais qu'elle a également immédiatement cessé d'utiliser le système d'enregistrement biométrique du temps de travail sans attendre une décision de la Chambre Contentieuse. Cela a permis de réduire la durée de la violation, qui aurait pu s'étendre sur toute la procédure.

257. La Chambre Contentieuse reconnaît que la première défenderesse a immédiatement cessé d'utiliser le système d'enregistrement biométrique du temps de travail, mais souligne qu'elle en a déjà tenu compte dans l'appréciation de la durée de la violation (voir ci-avant). Conformément aux Lignes directrices, chaque critère de l'article 83.2 du RGPD ne peut être

[55] EDPB - Lignes directrices 04/2022 sur le calcul des amendes administratives au titre du RGPD (V2.1, 24 mai 2023), p. 32.
[56] EDPB - Lignes directrices 04/2022 sur le calcul des amendes administratives au titre du RGPD (V2.1, 24 mai 2023), p. 33.

pris en compte qu'une seule fois dans le cadre de l'appréciation générale de l'article en question.[57]

258. **Toute autre circonstance aggravante ou atténuante applicable aux circonstances de l'espèce (article 82.3.k) du RGPD) -** La Chambre Contentieuse tient compte du fait qu'aucun profit financier ne découle du traitement en cause pour la première défenderesse, ce que la Chambre Contentieuse prend en compte en tant que circonstance atténuante lors de la détermination du montant de l'amende. La Chambre Contentieuse a également retenu comme autre circonstance le long délai entre la finalisation du rapport d'enquête et l'audition d'une part et (la publication de) la présente décision d'autre part. Cet élément a été considéré comme une circonstance atténuante en ce qui concerne le montant de l'amende.

259. La première défenderesse observe que ses chiffres d'affaires ont été pris en compte pour déterminer le niveau de l'amende dans le formulaire de sanction. Elle attire toutefois l'attention sur le fait que la société n'a pas réalisé de bénéfices depuis sa création en 2019, mais qu'elle enregistre même des pertes en raison de la nature des investissements. Dans la rédaction de la réponse au formulaire de sanction, la première défenderesse souligne que les comptes annuels 2023 n'étaient pas encore finalisés, mais que les perspectives financières n'étaient pas positives. Par conséquent, elle a dû procéder à une série de licenciements pour des raisons économiques fin 2023 et début 2024. La première défenderesse précise que son chiffre d'affaires est très élevé, compte tenu de la nature de ses investissements et de ses activités, à savoir la vente en gros à des professionnels. En revanche, ses bénéfices sont modestes, voire négatifs compte tenu de la conjoncture économique. La première défenderesse affirme qu'elle n'a pas encore atteint les résultats qu'elle visait lorsqu'elle a lancé ses activités en Belgique. En outre, elle génère un nombre important d'emplois en Flandre, dont certains pourraient être menacés par l'amende de 90.000 euros envisagée.

260. La Chambre Contentieuse souligne que, conformément aux lignes directrices de l'EDPB, elle est tenue de calculer le montant de l'amende envisagée sur la base du chiffre d'affaires de l'exercice précédent, aucune dérogation à cette méthode de calcul n'étant prévue. La Chambre Contentieuse reconnaît toutefois que l'environnement économique difficile et le fait que l'amende proposée mettrait en péril un nombre important d'emplois sont des facteurs atténuants dans cette affaire. À cet égard, la Chambre Contentieuse tient particulièrement compte du fait que la première défenderesse a reconnu la violation dès le début de la procédure et a assumé sa responsabilité en la matière tout au long de la présente procédure.

[57] EDPB - Lignes directrices 04/2022 sur le calcul des amendes administratives au titre du RGPD (V2.1, 24 mai 2023), p. 29.

261. **Autres circonstances atténuantes ou aggravantes** – D'autres circonstances ne s'appliquent pas dans cette affaire parce que les circonstances auxquelles il est fait référence ne se présentent pas en l'espèce.

ii) Influence sur le montant de l'amende

262. Ci-avant, le montant de départ concret a été fixé à 160.000 euros. Ensuite, d'éventuelles circonstances atténuantes ou aggravantes ont été examinées. La Chambre Contentieuse a estimé que plusieurs circonstances atténuantes pouvaient être prises en compte. Par conséquent, l'amende figurant dans le formulaire de sanction a été ajustée à 90.000 euros.

263. Suite aux éléments exposés ci-dessus, y compris les arguments avancés par la première défenderesse dans sa réponse au formulaire de sanction, la Chambre Contentieuse a décidé de réduire l'amende envisagée de 90.000 euros à 45.000 euros.

III.1.1.7. Étape 4 : Contrôle du dépassement des montants maximaux

264. Comme déjà exposé, une amende maximale de 4 % du chiffre d'affaires annuel mondial de l'entreprise s'applique à la violation constatée. Vu la marge brute de la première défenderesse (85.444.466 euros), le maximum légal de l'amende à infliger s'élève donc à 3.417.778,64 euros. Le montant de l'amende déterminé dans le formulaire de sanction pour les violations constatées a été fixé à 90.000 euros, ce qui est inférieur au montant maximum légal. Le montant réduit de l'amende de 45.000 euros est également bien inférieur au maximum légal susmentionné, de sorte qu'il n'y a pas de dépassement de ce maximum.

III.1.1.8. Étape 5 : Évaluation du caractère effectif, proportionné et dissuasif

265. En ce qui concerne le caractère disproportionné de l'amende proposée, dans sa réponse au formulaire de sanction, la première défenderesse se réfère à des décisions antérieures de la Chambre Contentieuse concernant le traitement de données biométriques, notamment celles concernant l'utilisation de caméras thermiques aux aéroports de Bruxelles-Zaventem et de Charleroi. La première défenderesse affirme que les amendes imposées par la Chambre Contentieuse ont été considérées comme disproportionnées par la Cour des marchés. Selon la première défenderesse, il est clair que les deux arrêts dans les affaires susmentionnées sont applicables à la présente affaire puisqu'elles concernent le traitement illicite de données biométriques. La première défenderesse estime que les points suivants sont particulièrement importants : (i) la première défenderesse ne fait pas de publicité marketing, contrairement aux aéroports dans les affaires précitées, et elle ne traite pas de données à caractère personnel dans le cadre de son activité principale, (ii) la première défenderesse n'a jamais enregistré l'empreinte digitale en tant que telle vu qu'elle est restée dans le système de la deuxième défenderesse et qu'elle a seulement reçu un code pour générer les informations relatives aux heures de travail, ce qui est fondamentalement

différent de la méthode utilisée à Brussels Airport, et (iii) le chiffre d'affaires de la première défenderesse est bien inférieur à celui des aéroports de Bruxelles et de Charleroi. Compte tenu de ces circonstances, le montant proposé de 90 000 euros serait disproportionné, selon la première défenderesse.

266. La Chambre Contentieuse rappelle tout d'abord que, conformément à l'article 83.2 du RGPD ainsi qu'aux Lignes directrices du Groupe 29 et aux Lignes directrices de l'EDPB en la matière, les amendes sont imposées "en fonction des circonstances du cas concret". En outre, la Chambre Contentieuse souligne à cet égard la jurisprudence de la Cour d'appel de Bruxelles, section Cour des marchés, selon laquelle "*le système juridique belge [n'attribue] pas de valeur de précédent contraignant ni aux décisions administratives, ni aux décisions judiciaires. Toute décision d'un juge (et il en va de même pour toute décision d'une autorité administrative, dès lors que le principe d'égalité n'est pas violé) est spécifique et ne s'applique pas à un autre cas que celui qui est traité*".[58] En ce qui concerne le montant de l'amende administrative imposée, la Cour des marchés a également souligné la marge d'appréciation de la Chambre Contentieuse : "*Cela signifie en pratique que l'APD peut non seulement décider de ne pas imposer d'amende au contrevenant mais aussi, si elle décide d'imposer une amende, de situer cette dernière entre le minimum, soit 1 EUR, et le maximum prévu. L'amende imposée est décidée par l'APD en tenant compte des critères énoncés par l'article 83, paragraphe 2 du RGPD" [Les citations de la Cour des marchés ont été traduites librement par le Secrétariat Général de l'Autorité, en l'absence de traduction officielle]. La Chambre Contentieuse n'est donc pas liée par les montants des amendes qu'elle a déjà infligées dans des affaires antérieures.*

267. Ensuite, la Chambre Contentieuse se réfère au fait que l'EDPB a publié des Lignes directrices sur le calcul des amendes administratives, ce qui n'était pas encore le cas lorsque les décisions précitées sur les caméras thermiques dans les aéroports ont été prises. Ces lignes directrices précisent le calcul de ces amendes à l'aide de différents facteurs à prendre en compte par la Chambre Contentieuse. Par conséquent, le calcul de l'amende administrative préalable à la publication des Lignes directrices de l'EDPB ne peut pas être comparé au calcul de l'amende administrative basé sur ces Lignes directrices.

268. En vertu de l'article 83.5, *ab initio* et sous b) du RGPD, la Chambre Contentieuse peut infliger une amende administrative pour les violations décrites ci-avant. Comme décrit dans les Lignes directrices, l'imposition d'une amende peut être considérée comme efficace si elle atteint les objectifs pour lesquels elle a été infligée. La Chambre Contentieuse constate que l'objectif est double : sanctionner un comportement illicite, d'une part, et promouvoir le respect des prescriptions en vigueur, d'autre part. La Chambre Contentieuse estime que l'exigence d'efficacité est remplie. En ce qui concerne la proportionnalité, la Chambre

[58] Cour d'appel de Bruxelles (section Cour des Marchés), NV N.D.P.K. c. APD, Arrêt 2021/AR/320 du 7 juillet 2021, p. 12.

Contentieuse se réfère à la nature, à la gravité et à la durée de la violation, ainsi qu'aux autres facteurs de l'article 83.2 du RGPD, tels qu'évalués aux points III.1.1.2 à III.1.1.6 de la présente décision. La mise en balance des facteurs précités combinée à la prise en compte du chiffre d'affaires de la première défenderesse amène la Chambre Contentieuse à constater que l'amende infligée répond à l'exigence de proportionnalité. Enfin, en termes de dissuasion, l'amende incite la première défenderesse à éviter toute récidive à l'avenir, et l'amende imposée a un effet dissuasif à l'égard des autres responsables du traitement.[59] Par conséquent, la Chambre Contentieuse estime que l'amende infligée de 45.000 euros répond aux exigences d'efficacité, de proportionnalité et de caractère dissuasif.

III.1.1.9. Autres griefs

269. La Chambre Contentieuse procède à un classement sans suite en ce qui concerne les autres griefs et constatations du Service d'Inspection car, sur la base des faits et des pièces du dossier, elle ne peut conclure qu'il soit question de violations du RGPD.

III.2. À l'égard de la deuxième défenderesse

270. La Chambre Contentieuse procède à un classement sans suite en ce qui concerne les griefs et constatations du Service d'Inspection à l'égard de la deuxième défenderesse car, sur la base des faits et des pièces du dossier, elle ne peut conclure qu'il soit question de violations du RGPD.

IV. Publication de la décision

271. 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.

[59] Le caractère dissuasif doit empêcher tant la première défenderesse que d'autres personnes de commettre la même violation à l'avenir, voir Comité européen de la protection des données (EDPB), Lignes directrices 04/2022 sur le calcul des amendes administratives au titre du RGPD (version 2.1), 24 mai 2023), point 142.

PAR CES MOTIFS,

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

- à l'égard de la première défenderesse :
  - en vertu de l'article 100, § 1er, 5° de la LCA, de réprimander la première défenderesse pour avoir omis de réaliser une AIPD (violation de l'**article 35 du RGPD**), pour avoir rédigé un registre des activités de traitement incomplet (violation de l'**article 30.1.a), b), c) et d) du RGPD**) et pour plusieurs violations du principe de responsabilité (**article 5.2 du RGPD**) ;
  - en vertu de l'article 100, § 1er, 5° de la LCA, d'avertir la première défenderesse pour l'avenir que le fait de répondre de manière incomplète à une demande d'accès constitue une violation de l'**article 12.1 *j°* l'article 15.1 du RGPD** ;
  - en vertu de l'article 100, § 1er, 13° de la LCA, conformément à l'article 83.2 du RGPD, d'infliger une amende administrative de 45.000 EUR suite à la violation de l'**article 5.1. a), b), et c), de l'article 9.1 *j°* l'article 6.1 et 9.2 et de l'article 13.1.c), d) et e) *j°* l'article 12.1 et l'article 5.2 du RGPD** ; et
  - en vertu de l'article 100, § 1er, 1° de la LCA, de classer sans suite les autres griefs et constatations étant donné qu'à cet égard, aucune violation ne peut être constatée ;
- en vertu de l'article 100, § 1er, 1° de la LCA, de classer sans suite les constatations étant donné qu'à cet égard, aucune violation ne peut être constatée.

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*[60]. La requête contradictoire doit être déposée au greffe de la Cour des marchés conformément à l'article 103 *quinquies* du

[60] *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.*

Code judiciaire[61], ou via le système informatique e-Deposit de la Justice (article 32*ter* du *Code judiciaire*).

(sé.) Hielke HIJMANS

Président de la Chambre Contentieuse

[61] *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.*