



Autorité de protection des données  
Gegevensbeschermingsautoriteit

## Chambre Contentieuse

### Décision quant au fond 24/2021 du 19 février 2021

**Numéro de dossier : DOS-2020-02716**

**Objet : Comptage des passants à des endroits spécifiques sur la digue et dans des zones commerçantes à la Côte au moyen de caméras intelligentes dans le cadre du Covid-19**

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

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

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

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

Vu les pièces du dossier ;

**a pris la décision suivante concernant :**

- Westtoer APB (Société provinciale autonome), dont le siège social se situe à Koning Albert I-laan 120 - 8200 SINT MICHIELS (BRUGES) et dont le numéro d'entreprise est le 0267.388.418, ci-après "le défendeur".

**1. Faits et procédure**

1. Le 9 juillet 2020, le Comité de direction de l'Autorité de protection des données décide, en vertu de l'article 63, 1° de la LCA, de saisir le Service d'Inspection d'un dossier car il a constaté des indices sérieux selon lesquels l'utilisation de caméras intelligentes par le défendeur pourrait entraîner une violation des principes fondamentaux de la protection des données à caractère personnel.
2. Plus précisément, il a été constaté que depuis le 27 juin 2020, plusieurs communes côtières avaient recours à des caméras intelligentes afin de mesurer l'affluence à certains endroits de la digue et dans des zones commerçantes de ces communes dans le cadre de l'épidémie de Covid-19. Le défendeur avait émis à cette fin un marché public au nom des communes côtières concernées, lequel a été attribué à la société X, qui est intervenue en tant que sous-traitant au sens de l'article 4.8 du RGPD.
3. Le 16 juillet 2020, en vertu de l'article 66, § 1<sup>er</sup>, 3° de la LCA, le Service d'Inspection adresse une demande écrite au défendeur afin d'obtenir des informations et de la documentation complémentaires sur l'activité de traitement susmentionnée, et plus précisément sur :
  - 1) le registre des activités de traitement tenu par le défendeur conformément à l'article 30 du RGPD ;
  - 2) le nombre de caméras intelligentes placées et actives dans le cadre du marché public "*Passantentellingen op specifieke locaties op de dijk en in winkelzones aan de Kust*" (Ndt : Comptages des passants à des endroits spécifiques sur la digue et dans des zones commerçantes à la Côte) émis par le défendeur ;
  - 3) le respect des principes de licéité, de loyauté et de transparence (article 5.1 a) du RGPD), de limitation des finalités (article 5.1 b) du RGPD) et de minimisation des données (article 5.1 c) du RGPD) ;
  - 4) le fondement juridique du traitement de données à caractère personnel via le système de caméras intelligentes au sens de l'article 6.1 du RGPD, lu conjointement avec les articles 5.2 et 24.1 du RGPD ;
  - 5) la réalisation d'une analyse d'impact relative à la protection des données (article 35 du RGPD) dans le cadre du marché public précité ; et

- 6) la désignation et la position du délégué à la protection des données (articles 37 et 38 du RGPD).
4. Le 13 août 2020, le Service d'Inspection adresse une lettre de rappel par e-mail au défendeur concernant le questionnaire écrit susmentionné.
5. Par e-mail du 18 août 2020, le défendeur informe le Service d'Inspection du fait que l'e-mail via lequel les réponses ainsi que les documents demandés ont été communiqués au Service d'Inspection ne lui est manifestement jamais parvenu.
6. Par e-mail du 18 août 2020, le défendeur transmet à nouveau au Service d'Inspection ses réponses aux questions de ce dernier ainsi que les documents demandés.

#### Le rapport d'inspection

7. Le 25 août 2020, le Service d'Inspection transmet son rapport d'inspection au président de la Chambre Contentieuse, conformément à l'article 91, § 2 de la LCA, suite à quoi la Chambre Contentieuse est saisie conformément à l'article 92, 3° de la LCA.

Dans son rapport, dans le cadre des indices sérieux, le Service d'Inspection formule les constatations suivantes :

- 1) Violation des articles 5.1 a) (principes de licéité, de loyauté et de transparence), b) (principe de limitation des finalités) et c) (principe de minimisation des données) du RGPD et de l'article 5.2 du RGPD (responsabilité) ; à cet égard, le Service d'Inspection déclare tout d'abord que le défendeur ne démontre pas suffisamment que les personnes concernées sont informées de manière loyale et transparente à propos du traitement de leurs données à caractère personnel via les caméras intelligentes et que le renvoi du défendeur à "*la déclaration de confidentialité figurant sur les sites Internet de Westtoer, dont dekust.be*" est trop vague et imprécis. [Ndt : tous les passages cités du dossier ont été traduits librement par le Service traduction de l'Autorité de protection des données, en l'absence de traduction officielle] Deuxièmement, le Service d'Inspection déclare que le défendeur ne démontre pas suffisamment que le traitement de données à caractère personnel via les caméras intelligentes en question a lieu pour des finalités déterminées, explicites et légitimes. Troisièmement, le Service d'Inspection déclare que le défendeur ne démontre pas suffisamment que les données à caractère personnel traitées via les caméras intelligentes sont adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées.

- 2) Violation de l'article 6.1 du RGPD : le Service d'Inspection constate que le défendeur fonde le traitement de données à caractère personnel au moyen de caméras intelligentes sur l'article 6.1 e) du RGPD et qu'il se réfère à cet égard au contrat de gestion conclu avec la province de Flandre occidentale, dans lequel il est précisé que la mission du défendeur consiste à soutenir le tourisme en Flandre occidentale. Le Service d'Inspection estime toutefois que le défendeur ne démontre pas pourquoi la réalisation de cette mission d'intérêt public nécessite de traiter des données à caractère personnel via des caméras intelligentes. À cet égard, le Service d'Inspection attire l'attention sur le fait que la capacité de démontrer cette nécessité est une exigence en vertu de l'article 6.1 e) du RGPD lu conjointement avec les articles 5.2 et 24.1 du RGPD.
- 3) Violation des articles 12.1, 12.6, 13.1 et 13.2 du RGPD : le Service d'Inspection constate que les informations fournies par le défendeur via la déclaration de confidentialité publiée sur le site Internet [www.westtoer.be/nl/dataverwerking](http://www.westtoer.be/nl/dataverwerking) ne sont pas entièrement correctes ni transparentes.
- 4) Violation de l'article 35.2 et 35.7 du RGPD : le Service d'Inspection constate que l'analyse d'impact relative à la protection des données effectuée par le défendeur ne répond pas aux exigences reprises dans les articles susmentionnés et que le délégué à la protection des données n'y a pas été suffisamment associé.

En outre, le Service d'Inspection formule plusieurs constatations complémentaires *en dehors du cadre* des indices sérieux, à savoir concernant :

- 1) une violation de l'article 4.11 du RGPD lu conjointement avec l'article 6.1 a) du RGPD ainsi que des articles 7.1 et 7.3 du RGPD : le Service d'Inspection constate en particulier que sur le site Internet du défendeur, la poursuite de la navigation sur ce site Internet par la personne concernée est considérée comme un consentement à l'utilisation de cookies.
- 2) une violation de l'article 30.1 du RGPD : le Service d'Inspection constate que le registre des activités de traitement du défendeur ne répond pas aux exigences de l'article susmentionné. Plus précisément, le Service d'Inspection constate que :
  - i) les coordonnées du responsable du traitement sont incomplètes, vu que l'adresse e-mail mentionnée dans la déclaration de confidentialité du défendeur n'y est pas reprise ;

- ii) la description des catégories de personnes concernées est incomplète, au vu de la mention "autres" dans la colonne "catégories de personnes physiques" ;
  - iii) les pays tiers vers lesquels des données à caractère personnel sont transférées ne sont pas mentionnés, mais seulement le traitement d'adresses e-mail via Mailchimp, sans mentionner les pays dont il s'agit ; et
  - iv) le registre ne mentionne pas les visiteurs du site Internet ni l'utilisation de cookies.
- 3) Pas de violation des articles 37.5 et 37.7 du RGPD concernant la désignation du délégué à la protection des données.
- 4) Violation des articles 38.2 et 38.3 du RGPD et pas de violation de l'article 38.6 du RGPD : le Service d'Inspection constate que le délégué à la protection des données n'est pas occupé à temps plein et que ce dernier ne fait pas rapport directement au niveau le plus élevé de la direction du défendeur.

8. Le 3 septembre 2020, la Chambre Contentieuse décide, en vertu de l'article 95, § 1<sup>er</sup>, 1<sup>o</sup> et de l'article 98 de la LCA, que le dossier peut être traité sur le fond.

9. Par courrier du 3 septembre 2020, le défendeur est informé du fait que le dossier peut être traité sur le fond et, en vertu de l'article 99 de la LCA, il est également informé du délai pour introduire ses conclusions.

#### Conclusions en réponse du défendeur

10. Le 1<sup>er</sup> octobre 2020, le défendeur dépose ses conclusions en réponse et demande également à être entendu, conformément à l'article 98, 2<sup>o</sup> de la LCA.

11. Dans ses conclusions en réponse, le défendeur déclare en ce qui concerne la première constatation du Service d'Inspection (violation des principes de licéité, de loyauté et de transparence (art. 5.1 a) du RGPD), de limitation des finalités (art. 5.1 b) du RGPD) et de minimisation des données (art. 5.1 c) du RGPD) que cette constatation est inexacte en droit comme en fait, vu que le défendeur a suffisamment informé les personnes concernées à propos du traitement de leurs données à caractère personnel, et ce via la déclaration de confidentialité reprise sur les sites Internet du demandeur - dont [www.dekust.be](http://www.dekust.be) - d'une part et via l'importante couverture dans la presse et la publication d'un communiqué de presse d'autre part. Le défendeur en joint les pièces justificatives et conclut que, vu cette importante

communication, on peut supposer que la grande majorité des visiteurs de la côte étaient au courant de l'utilisation des caméras intelligentes.

12. Le défendeur ajoute que contrairement à ce qui a été constaté par le Service d'Inspection, le système de comptage des passants vise bel et bien une finalité déterminée, explicite et légitime, à savoir contrôler le nombre et la concentration de visiteurs à la côte dans le cadre de la lutte contre la pandémie de Covid-19.
13. En ce qui concerne le respect du principe de minimisation des données, le défendeur affirme dans ses conclusions en réponse avoir préalablement effectué une analyse approfondie avec le sous-traitant ainsi que son délégué à la protection des données afin de garantir que l'utilisation des caméras intelligentes en question soit adéquate, pertinente et limitée à ce qui est nécessaire au regard de la finalité visée. Le défendeur précise que les mesures suivantes ont été prises afin de limiter autant que possible le traitement de données : i) l'anonymisation des données à caractère personnel, ii) le délai de conservation court des données à caractère personnel, iii) la limitation du nombre et du placement des caméras, iv) le délai court de la mesure et v) l'accès limité aux données à caractère personnel.
14. Le défendeur explique en outre en ce qui concerne la *nécessité* de l'utilisation du système de caméras intelligentes que les systèmes de surveillance alternatifs - tels que des comptages manuels ou des comptages à l'aide de signaux wi-fi - ne sont pas assez précis pour la finalité visée et que seul le système utilisé permet d'obtenir certaines informations supplémentaires qui sont nécessaires à la réalisation de cette finalité. Le défendeur affirme plus précisément que le respect ou non des règles de distanciation sociale, le sens de circulation des passants et les différents types de passants ne peuvent être constatés par aucun système alternatif et que seul le système de caméras intelligentes permet un rapport en temps réel, ce qui est crucial pour pouvoir communiquer et, le cas échéant, intervenir en temps opportun.
15. En ce qui concerne la deuxième constatation du Service d'Inspection (licéité du traitement - article 6.1 du RGPD), le défendeur soutient que le système de comptage des passants était bel et bien nécessaire pour accomplir la mission d'intérêt public au sens de l'article 6.1 e) du RGPD, à savoir lutter contre la pandémie de Covid-19 et assurer la sécurité des visiteurs de la Côte. Le défendeur se réfère à cet égard au contrat de gestion avec la province de Flandre occidentale. Il déclare plus précisément que le système de caméras intelligentes était le seul moyen d'accomplir la mission d'intérêt public susmentionnée, vu que i) seul un comptage via des caméras intelligentes permet de fournir des données suffisamment précises sur le nombre de visiteurs, ii) seul un comptage via des caméras intelligentes permet d'obtenir des informations complémentaires cruciales et iii) seul ce système permet de faire un rapport en temps réel.

16. En ce qui concerne les constatations du Service d'Inspections relatives à la transparence (articles 12 et 13 du RGPD), le défendeur reconnaît que la déclaration de confidentialité peut être améliorée, mais il déclare ne pas être d'accord avec les accusations.
17. En ce qui concerne les constatations du Service d'Inspection quant à l'analyse d'impact relative à la protection des données (articles 35.2 et 35.7 du RGPD), le défendeur soutient que l'avis du délégué à la protection des données a bel et bien été recueilli et que cet avis reprend bien les mentions obligatoires de l'article 35.7 du RGPD ; le défendeur en joint des justificatifs.
18. En ce qui concerne les constatations du Service d'Inspection relatives au consentement aux cookies sur le site Internet du défendeur (articles 4.1, 6.1 a) et 7.1 du RGPD), ce dernier reconnaît que la politique en matière de cookies peut être améliorée mais il affirme qu'il est expliqué dans la déclaration de confidentialité comment les cookies peuvent être supprimés, en précisant que cela est possible via les paramètres du navigateur.
19. En ce qui concerne les constatations du Service d'Inspection relatives au registre des activités de traitement (article 30.1 du RGPD), le défendeur soutient que l'on ne peut pas affirmer que les coordonnées de Westtoer sont incomplètes uniquement en raison de l'absence de l'adresse e-mail [dataverwerking@westtoer.be](mailto:dataverwerking@westtoer.be).
20. En ce qui concerne les constatations du Service d'Inspection relatives à la position du délégué à la protection des données (articles 38.2 et 38.3 du RGPD), le défendeur affirme que le fait que ce dernier exerce sa fonction selon un régime de 4/5 n'implique pas qu'il n'ait pas assez de temps pour exercer ses fonctions. Le défendeur souligne à cet égard que le Groupe de travail "Article 29" sur la protection des données a précisé qu'un délégué à la protection des données ne devait pas nécessairement exercer ses missions à temps plein. Le défendeur nie cette accusation et affirme que les actes du délégué dans ce dossier concernant le système de comptage des passants, et notamment l'avis de celui-ci, confirment que le délégué à la protection des données dispose bel et bien de suffisamment de temps pour accomplir ses tâches. Enfin, le défendeur confirme que pour sa communication journalière, le délégué dispose d'une ligne avec un collaborateur de Westtoer, mais que ce dernier a le droit et l'obligation de partager des points importants avec la hiérarchie de Westtoer.
21. Par courrier du 9 décembre 2020, la Chambre Contentieuse adresse plusieurs questions complémentaires au défendeur en vue de l'audition.
22. Le 15 décembre 2020, le défendeur transmet ses réponses écrites aux questions susmentionnées de la Chambre Contentieuse.

### L'audition

23. Le 16 décembre 2020, le défendeur est entendu par la Chambre Contentieuse, conformément à l'article 53 du règlement d'ordre intérieur.
24. Pendant cette audition, le défendeur fait à la Chambre Contentieuse une démonstration visuelle du fonctionnement du système des caméras intelligentes utilisé à titre de système de comptage des passants.
25. Le 5 janvier 2021, le procès-verbal d'audition est transmis au défendeur, conformément à l'article 54 du règlement d'ordre intérieur.
26. Le 8 janvier 2021, le défendeur informe la Chambre Contentieuse qu'il n'a aucune remarque concernant le procès-verbal d'audition susmentionné.

## **2. Motivation**

### 2.1. "Traitement de données à caractère personnel" et la compétence de la Chambre Contentieuse

27. L'article 4.1 du RGPD définit la notion de "données à caractère personnel" comme étant *"toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée "personne concernée") ; est réputée être une "personne physique identifiable" une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale"*.
28. Conformément à l'article 4.2 du RGPD, il y a lieu de considérer comme un *"traitement"* de données à caractère personnel : *"toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction"*.

29. La Cour de justice a confirmé à plusieurs reprises dans sa jurisprudence que la prise d'images de personnes par des caméras relevait de la notion de "donnée à caractère personnel" au sens des normes de droit européen en matière de protection des données. Dans son arrêt **Ryneš**, la Cour de justice a précisé à cet égard :

*"Il convient de rappeler que [...] cette directive [...] s'applique "au traitement de données à caractère personnel, automatisé en tout ou en partie, ainsi qu'au traitement non automatisé de données à caractère personnel contenues ou appelées à figurer dans un fichier".*

*La notion de "données à caractère personnel" [...] englobe [...] "toute information concernant une personne physique identifiée ou identifiable". 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".*

*Une image d'une personne prise par une caméra relève dès lors de la notion de données à caractère personnel au sens de la disposition visée au point précédent, vu qu'elle permet d'identifier la personne en question."*<sup>2</sup>

30. En l'espèce, il ressort des pièces du dossier ainsi que des explications fournies par le défendeur lors de l'audition que l'activité en question concerne un système de comptage des passants où, grâce à l'utilisation de ce que l'on appelle des "caméras intelligentes", les passants sont filmés et où les images vidéos concernées sont ensuite conservées localement de façon temporaire (c.-à-d. pendant moins d'une seconde), pour ensuite être brouillées et envoyées au data center du sous-traitant.

31. Sur la base de ce qui précède, la Chambre Contentieuse constate *qu'en l'occurrence*, il est question d'un traitement de données à caractère personnel au sens de l'article 4.1 *juncto* /article 4.2 du RGPD et que l'Autorité de protection des données est par conséquent compétente pour contrôler ce traitement et la Chambre contentieuse pour prendre une décision en la matière.

## 2.2. Identification du responsable du traitement (article 4.7 du RGPD)

32. Conformément à l'article 4.7 du RGPD, il y a lieu de considérer comme le responsable du traitement : la "*personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement*".

<sup>1</sup> Directive 95/46/CE, abrogée et remplacée par le RGPD.

<sup>2</sup> Arrêt CJUE du 11 décembre 2014, Ryneš, C-212/13, ECLI:EU:C:2014:2428, considérants 20-22 (soulignement par la Chambre Contentieuse).

33. La Cour de justice a, à plusieurs reprises, interprété la notion de "responsable du traitement" de manière large dans sa jurisprudence afin d'assurer une protection efficace et complète des personnes concernées.<sup>3</sup>
34. Conformément à l'Avis 1/2010 du Groupe 29, la qualité du *(des) responsable(s) du traitement concerné(s) doit être concrètement évaluée.*<sup>4</sup>
35. En l'espèce, la Chambre Contentieuse constate tout d'abord que le défendeur a effectué un traitement de données à caractère personnel au sens de l'article 4.2 du RGPD, à savoir *"toute opération ou ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensemble de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation, ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction"*. Comme expliqué ci-dessus, le défendeur traite des images vidéos de passants, prises à l'aide de caméras. Le fait que ce traitement ne soit effectué que pour une courte durée ne change rien au fait qu'il relève du champ d'application matériel du RGPD. Il s'agit en effet en l'occurrence d'un *"traitement automatisé en tout ou en partie"* au sens de l'article 2 du RGPD.
36. Toujours selon l'Avis 1/2010 du Groupe 29, les notions "les finalités" et "les moyens" doivent être examinées ensemble de manière indissociable et il convient à cet égard d'établir qui détermine le "pourquoi" (les finalités) et le "comment" (les moyens) du traitement.<sup>5</sup>
37. La Chambre Contentieuse constate en outre que le défendeur a défini les finalités et les moyens du traitement de données à caractère personnel concerné, vu que ce dernier a émis en tant que pouvoir adjudicateur le marché public de services ayant pour objet *"Comptage des passants à des endroits spécifiques sur la digue et dans des zones commerçantes à la Côte"*, en y spécifiant les finalités et les moyens du traitement en question.
38. En outre, un contrat de sous-traitance a été conclu entre le défendeur et le sous-traitant le 17 juin 2020, conformément à l'article 28 du RGPD, dans lequel le premier est désigné

---

<sup>3</sup> Voir notamment CJUE, 5 juin 2018, C-210/16 - Wirtschaftsakademie Schleswig-Holstein, ECLI:EU:C:2018:388, considérants 27-29.

<sup>4</sup> Voir Groupe 29, Avis 1/2010 sur les notions de "responsable du traitement" et de "sous-traitant", 16 février 2010 (WP 169), telles que précisées par l'APD dans une note "Le point sur les notions de responsable de traitement / sous-traitant au regard du Règlement (UE) n° 2016/679 du Parlement européen et du Conseil du 27 avril 2016 sur la protection des données à caractère personnel (RGPD) et quelques applications spécifiques aux professions libérales telles que les avocats".

<sup>5</sup> Groupe 29, Avis 1/2010 sur les notions de "responsable de traitement" et de "sous-traitant", WP 169, p. 15.

comme étant le responsable du traitement.<sup>6</sup> Le défendeur reconnaît également lui-même être le responsable du traitement.

39. Sur la base de ce qui précède, la Chambre Contentieuse conclut que le défendeur doit être considéré comme responsable du traitement au sens de l'article 4.7 du RGPD pour le traitement de données à caractère personnel faisant l'objet de l'enquête. Vu le principe de la responsabilité prévu aux articles 5.2 et 24 du RGPD, il est par conséquent, en cette qualité, tenu de garantir le respect des principes et des dispositions du RGPD.

2.3. En ce qui concerne les constatations du Service d'Inspection dans le cadre des indices sérieux

40. La Chambre Contentieuse constate que les constatations B.1 et B.2 du Service d'Inspection concernent la licéité du système de comptage des passants au moyen de caméras intelligentes en tant que tel, alors que les autres constatations *dans le cadre* des indices sérieux concernent la déclaration de confidentialité et l'analyse d'impact relative à la protection des données. La Chambre Contentieuse examinera les constatations susmentionnées séparément.

2.3.1. Le respect des principes relatifs au traitement de données à caractère personnel (articles 5.1 et 5.2 du RGPD) et la licéité du traitement (articles 6.1 du RGPD)

41. Dans ses constatations B.1 et B.2, le Service d'Inspection constate que le défendeur n'aurait pas suffisamment démontré que le système de caméras intelligentes utilisé respecte les principes relatifs à la protection des données. Le Service d'Inspection déclare plus précisément que le défendeur aurait commis une violation des articles 5.1 a) (licéité, loyauté et transparence), 5.1 b) (limitation des finalités) et 5.1 c) (minimisation des données) du RGPD ainsi que des articles 5.2 (responsabilité) et 6.1 (licéité du traitement) du RGPD.

42. En ce qui concerne les constatations susmentionnées du Service d'Inspection, la Chambre Contentieuse attire l'attention sur le fait que l'utilisation de caméras dites intelligentes dans l'espace public n'est conforme aux normes de droit européen en matière de protection des données que si et dans la mesure où les principes suivants sont respectés :

---

<sup>6</sup> D'après les pièces du défendeur.

**A. Le traitement des données à caractère personnel via le système de caméras intelligentes doit reposer sur un motif de licéité valable au sens de l'article 6 du RGPD**

43. Comme cela vaut pour tout traitement de données à caractère personnel, le traitement de données à caractère personnel au moyen de caméras intelligentes n'est tout d'abord licite que s'il se déroule conformément à l'article 6.1 du RGPD et notamment si et dans la mesure où au moins l'une des conditions suivantes est remplie :

- a) *"la personne concernée a consenti au traitement de ses données à caractère personnel pour une ou plusieurs finalités spécifiques ;*
- b) *le traitement est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci ;*
- c) *le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis ;*
- d) *le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique ;*
- e) *le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement ;*
- f) *le traitement est nécessaire aux fins des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers, à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne concernée qui exigent une protection des données à caractère personnel, notamment lorsque la personne concernée est un enfant."*

44. Si des catégories particulières de données à caractère personnel - telles que des données relatives à la santé des personnes concernées - sont traitées via le système, le responsable du traitement doit également démontrer qu'un des motifs d'exception de l'article 9.2 du RGPD s'applique. En l'occurrence, cela n'est toutefois pas démontré.

45. Conformément aux Lignes directrices 3/2019 en la matière du Comité européen de la protection des données (ci-après désigné par l'abréviation anglaise : "EDPB"), en principe tout fondement juridique prévu à l'article 6.1 du RGPD peut constituer une base juridique pour le traitement de données à caractère personnel obtenues via des images vidéo. L'EDPB précise néanmoins que dans la pratique, un tel traitement se fondera généralement sur l'article 6.1 f) du RGPD (intérêt légitime) ou sur l'article 6.1 e) du RGPD (nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique).

Dans des cas plutôt exceptionnels, l'article 6.1 a) du RGPD (consentement) peut être utilisé comme base juridique par le responsable du traitement.<sup>7</sup>

46. En l'espèce, il ressort des conclusions en réponse du défendeur, du registre des activités de traitement tenu par ce dernier ainsi que de l'analyse d'impact relative à la protection des données qu'il a effectuée qu'il fonde le traitement de données à caractère personnel en question sur l'article 6.1 e) du RGPD. Le défendeur déclare plus spécifiquement que sa mission d'intérêt public consiste à soutenir et à promouvoir le tourisme en Flandre occidentale et précise que cela implique que ce tourisme puisse se faire en toute sécurité. Il se réfère à cet égard au contrat de gestion conclu avec la province de Flandre occidentale pour la période 2020-2024.<sup>8</sup> Le défendeur précise que le système de comptage des passants au moyen de caméras intelligentes avait pour but de lutter contre la pandémie de Covid-19 et de préserver la sécurité des visiteurs de la Côte.

47. La Chambre Contentieuse souligne que le recours au motif de licéité repris à l'article 6.1 e) du RGPD implique que le responsable du traitement doit pouvoir démontrer que :

- i) celui-ci est chargé d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique ; et que
- ii) le traitement en question *est nécessaire* à l'accomplissement de la tâche susmentionnée (voir aussi ci-après le point B).

48. En ce qui concerne le point (i), le considérant 45 du RGPD et l'article 6.3 du RGPD précisent qu'un traitement fondé sur l'article 6.1 e) du RGPD "*devrait avoir un fondement dans le droit de l'Union ou dans le droit d'un État membre*". Le RGPD exclut ainsi qu'une "*mission d'intérêt public*" ou "*relevant de l'exercice de l'autorité publique*" soit confiée au responsable du traitement en vertu d'un contrat, même si ce contrat était conclu dans l'intérêt public<sup>9</sup>.

49. En ce qui concerne ce fondement qu'un traitement basé sur l'article 6.1 e) devrait avoir "*dans le droit de l'Union ou dans le droit d'un État membre*", le considérant 45 du RGPD ajoute en outre ceci :

---

<sup>7</sup> EDPB, Lignes directrices 3/2019 (version 2.0) sur le traitement des données à caractère personnel par des dispositifs vidéo, disponibles via ce lien : [https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32019-processing-personal-data-through-video\\_fr](https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32019-processing-personal-data-through-video_fr) (ci-après les Lignes directrices 3/2019), point 16.

<sup>8</sup> Pièces du défendeur.

<sup>9</sup> KOTCHY, W., "Article 6. Lawfulness of processing" in KUNER, C., BYGRAVE, L.A. et DOCKSEY, C., *The EU General Data Protection Regulation (GDPR). A commentary*, Oxford University Press, Oxford, p. 335.

*"Il devrait également appartenir au droit de l'Union ou au droit d'un État membre de déterminer la finalité du traitement. Par ailleurs, ce droit pourrait préciser les conditions générales du présent règlement régissant la licéité du traitement des données à caractère personnel, établir les spécifications visant à déterminer le responsable du traitement, le type de données à caractère personnel faisant l'objet du traitement, les personnes concernées, les entités auxquelles les données à caractère personnel peuvent être communiquées, les limitations de la finalité, la durée de conservation et d'autres mesures visant à garantir un traitement licite et loyal. Il devrait, également, appartenir au droit de l'Union ou au droit d'un État membre de déterminer si le responsable du traitement exécutant une mission d'intérêt public ou relevant de l'exercice de l'autorité publique devrait être une autorité publique ou une autre personne physique ou morale de droit public (...) "[Soulignement par la Chambre Contentieuse].*

50. Le considérant 45 du RGPD précise toutefois qu'une disposition légale spécifique n'est pas requise pour chaque traitement *individuel*. Une législation faisant office de base pour *plusieurs* traitements qui sont nécessaires à l'accomplissement d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique peut par conséquent suffire.
51. Dans le cas présent, le responsable du traitement se réfère au contrat de gestion conclu avec la province de Flandre occidentale comme base pour sa mission d'intérêt public au sens de l'article 6.1 e) du RGPD et pour sa mission décrite dans ce contrat (*voir ci-avant*). Dans son analyse d'impact relative à la protection des données<sup>10</sup>, le défendeur précise que "*la base juridique pour ce traitement se trouve dans les missions d'intérêt public et d'autorité publique des pouvoirs locaux*"<sup>11</sup>.
52. La Chambre Contentieuse attire l'attention sur le fait que l'une des missions d'intérêt public *des pouvoirs* locaux (c.-à-d. les communes) consiste en effet à garantir la sécurité des personnes sur leur territoire (voir notamment l'article 135, § 2 de la Nouvelle loi communale). Elle constate que, dans le cas présent, *le* défendeur ne mentionne toutefois pas quel est le fondement légal précis en droit européen ou en droit belge qui justifie le traitement litigieux.
53. Conformément à l'article 6.3 du RGPD, comme déjà "indiqué, "*la finalité du traitement doit être définie dans ce fondement juridique ou, en ce qui concerne le traitement visé au*

---

<sup>10</sup> Pièces du défendeur.

<sup>11</sup> AIPD du défendeur, p. 5.

*paragraphe 6.1, point e), il doit être nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement".*

54. Par ailleurs, aux termes de l'article 6.3 du RGPD, le fondement juridique peut aussi *"contenir des dispositions spécifiques pour adapter l'application des règles du présent règlement, entre autres: les conditions générales régissant la licéité du traitement par le responsable du traitement; les types de données qui font l'objet du traitement; les personnes concernées; les entités auxquelles les données à caractère personnel peuvent être communiquées et les finalités pour lesquelles elles peuvent l'être; la limitation des finalités; les durées de conservation; et les opérations et procédures de traitement (...)"*.
55. À cet égard, la Chambre Contentieuse se réfère également aux avis sur la législation de l'Autorité de protection des données (Centre de connaissances) - par exemple concernant certaines mesures prises dans le cadre de la lutte contre la propagation du coronavirus sur la base de l'article 6.1 e) du RGPD - dans lesquels il est également souligné que conformément à l'article 6.3 susmentionné du RGPD, lu conjointement avec l'article 22 de la *Constitution* et l'article 8 de la CEDH, une norme de rang législatif doit déterminer les caractéristiques essentielles d'un traitement de données nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement. Dans les avis susmentionnés, il est souligné à cet égard que le traitement en question doit *être encadré par* une norme qui soit suffisamment *claire et précise* et dont l'application soit *prévisible* pour les personnes concernées. Dans ce contexte, il est précisé que cette norme doit reprendre en particulier les éléments suivants : la ou les finalité(s) précise(s) du traitement ; l'identité du (ou des) responsable(s) du traitement ; les catégories de données traitées, étant entendu que celles-ci doivent s'avérer – conformément à l'article 5.1 du RGPD, *"adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées"* ; les catégories de personnes concernées dont les données seront traitées ; la durée de conservation des données ; les destinataires ou catégories de destinataires auxquels leurs données sont communiquées et les circonstances dans lesquelles et les raisons pour lesquelles elles seront communiquées ainsi que l'éventuelle limitation des obligations et/ou des droits visé(e)s au articles 5, 12 à 22 inclus et 34 du RGPD.<sup>12</sup>
56. À cet égard, la Chambre Contentieuse souligne toutefois que les missions d'intérêt public ou relevant de l'exercice de l'autorité publique dont sont investis les responsables du traitement ne sont souvent pas basées sur des obligations ou des normes législatives circonscrites avec précision répondant aux exigences mentionnées au point 55, plus précisément la définition

<sup>12</sup> Voir e.a. les avis 36/2020, 42/2020, 44/2020, 52/2020 et 64/2020 (<https://www.autoriteprotectiondonnees.be/citoyen/chercher>).

des caractéristiques essentielles du traitement de données. Les traitements s'effectuent plutôt sur la base d'une autorisation plus générale d'agir dans la mesure nécessaire à l'accomplissement de la mission - comme, dans le cas présent, la sécurité et la santé des habitants et des touristes dans les communes côtières.<sup>13</sup> Il s'agit souvent de législations relativement anciennes où l'aspect de la protection des données n'a pas encore été suffisamment développé. Il en résulte que dans la pratique, la base légale en question ne contient souvent aucune disposition décrivant concrètement les traitements de données nécessaires. Les responsables du traitement qui souhaitent invoquer l'article 6.1 e), du RGPD sur la base d'une telle base légale doivent alors effectuer eux-mêmes une pondération entre la nécessité du traitement pour la mission d'intérêt public et les intérêts des personnes concernées.

57. Dans le cas présent, la Chambre Contentieuse constate donc que le défendeur démontre de manière plausible qu'il poursuit une mission d'intérêt public au sens de l'article 6.1 e) du RGPD. Il convient toutefois de constater que le défendeur lui-même n'indique pas sur quelle base légale spécifique (telle que l'article 135, § 2 de la Nouvelle loi communale) dans le droit de l'Union ou le droit d'un État membre au sens de l'article 6.3 du RGPD l'activité de traitement en question - à savoir le traitement de données à caractère personnel via un système de caméras intelligentes dans le cadre de la lutte contre le Covid-19 - est fondée.
58. Il incombe évidemment en premier lieu aux pouvoirs publics à la demande desquels le traitement a lieu - en l'occurrence la province de Flandre occidentale et les communes côtières concernées - de veiller à ce qu'il existe une base légale répondant aux exigences de l'article 6.3 du RGPD. Ceci n'empêche pas qu'il incombe également à un responsable du traitement tel que le défendeur de vérifier dans quelle mesure il existe une base légale suffisante.
59. Dans la présente décision, la Chambre Contentieuse se limite à ces considérations générales à propos du fondement juridique. Elle n'a pas examiné la présence d'un fondement juridique ad hoc pour les traitements en question par Westtoer. Elle attire l'attention sur le fait qu'une analyse complète du fondement juridique nécessiterait également d'y associer la province ainsi que toutes les communes concernées. Ceci augmenterait considérablement la complexité de l'analyse par la Chambre Contentieuse. Vu la grande importance sociale d'une décision en temps opportun de la Chambre Contentieuse qui fixe des conditions strictes en vue d'éventuels futurs comptages de passants, cette analyse n'a pas été effectuée dans le cadre de la présente décision.

---

<sup>13</sup> KOTCHY, W., "Article 6. Lawfulness of processing" in KUNER, C., BYGRAVE, L.A. et DOCKSEY, C., *The EU General Data Protection Regulation (GDPR). A commentary*, Oxford University Press, Oxford, p. 336.

60. La Chambre Contentieuse souligne néanmoins que pour d'éventuelles activités de traitement similaires futures, le défendeur et les autres responsables du traitement doivent veiller à ce que les conditions de l'article 6.1 e) du RGPD *juncto* l'article 6.3 du RGPD soient remplies, conformément à la responsabilité reprise à l'article 5.2 du RGPD. Dans une prochaine décision concernant des mesures dans le cadre de la crise sanitaire, la Chambre Contentieuse peut aussi examiner la justesse du fondement juridique.

**B. La nécessité et la proportionnalité de la mesure doivent être démontrées par rapport aux finalités visées par l'utilisation de caméras intelligentes**

61. Outre l'exigence que le traitement de données à caractère personnel au moyen de caméras intelligentes puisse uniquement avoir lieu moyennant un motif de licéité valable, il convient en outre de démontrer que l'utilisation du système est nécessaire (ii; voir ci-avant le point 47) et que cela n'implique pas d'atteinte disproportionnée au droit à la protection des données des personnes concernées. Cette exigence de nécessité figure dans plusieurs dispositions du RGPD, notamment l'article 5.1 c) (principe de minimisation des données) et les articles 6.1 c) et 6.1 e) du RGPD.

62. Le test de nécessité et de proportionnalité est encore plus important si le responsable du traitement fonde le traitement concerné, comme c'est le cas en l'espèce, sur cette dernière disposition, l'article 6.1 e) du RGPD. Contrairement à l'article 6.1 c) du RGPD (obligation légale à laquelle le responsable du traitement est soumis), la mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement ne se traduira en effet souvent pas - comme déjà indiqué ci-avant - par des obligations décrites avec précision, mais plutôt par une autorisation plus générale d'agir dans la mesure nécessaire à l'accomplissement de la mission, comme en l'espèce préserver la sécurité et la santé des habitants et des touristes de la Côte.<sup>14</sup>

63. Il en découle que le responsable du traitement doit, le cas échéant, effectuer une certaine pondération entre la nécessité visée dans l'article susmentionné et les intérêts des personnes concernées. À cet égard, il convient de souligner, en ce qui concerne cette pondération des intérêts, que l'article 6.1 e) du RGPD ne diffère pas fondamentalement en substance de l'article 6.1 f) du RGPD (intérêt légitime). L'élément précité de pondération des intérêts explique également le droit d'opposition repris à l'article 21 du RGPD, qui vaut uniquement pour les traitements fondés sur ces deux motifs de licéité.

---

<sup>14</sup> KOTCHY, W., "Article 6. Lawfulness of processing" in KUNER, C., BYGRAVE, L.A. et DOCKSEY, C., *The EU General Data Protection Regulation (GDPR). A commentary*, Oxford University Press, Oxford, p. 336.

64. La Chambre Contentieuse attire l'attention sur le fait qu'il convient d'évaluer notamment la nécessité et que la pondération expliquée ci-avant doit être effectuée à la lumière de la jurisprudence de la Cour de justice de l'Union européenne ainsi que de l'article 8 de la Convention européenne des droits de l'homme (CEDH) et de l'article 22 de la Constitution belge, ainsi que la gravité de l'ingérence dans la vie privée des personnes concernées.
65. Dans sa jurisprudence - notamment dans l'arrêt *Huber* -, la Cour de justice de l'Union Européenne souligne à cet égard que le concept de "nécessité" au sens de l'article 6.1 e) du RGPD doit être interprété de façon stricte et être évalué à la lumière de la proportionnalité et que, en d'autres termes, si plusieurs alternatives existent pour atteindre la finalité visée, il convient d'opter pour la moins intrusive.<sup>15</sup>
66. Le caractère nécessaire et proportionné de la mesure doit par conséquent être plus précisément démontré en ce qui concerne l'absence de moyens moins intrusifs pour les droits et libertés des personnes concernées via lesquels les finalités visées pourraient également être atteintes.
67. En ce qui concerne la nécessité du système de caméras intelligentes qu'il utilise, le défendeur affirme dans ses conclusions en réponse ainsi que pendant l'audition tout d'abord que ce système de comptage des passants était la seule manière de lutter efficacement contre la pandémie de Covid-19 et donc d'accomplir sa mission d'intérêt public et ce pour les raisons suivantes :
- i. seul un comptage via des caméras intelligentes peut fournir des données suffisamment précises sur le nombre de visiteurs. Le défendeur précise à ce sujet que les flux de visiteurs sont complexes et que seul le système des caméras intelligentes peut mesurer de tels flux de visiteurs avec suffisamment de précision, alors que les systèmes de surveillance alternatifs sont beaucoup moins précis ;
  - ii. seul un comptage via des caméras intelligentes peut fournir des informations supplémentaires cruciales. Le défendeur déclare à ce propos qu'afin de prendre des décisions appropriées, il convient d'obtenir des informations supplémentaires, comme notamment le sens des flux de visiteurs ; et
  - iii. que seul un comptage via des caméras intelligentes permet le rapport en temps réel nécessaire. Le défendeur précise à cet égard qu'afin de pouvoir intervenir immédiatement s'il le faut, il est nécessaire de pouvoir effectuer un rapport en temps réel et que seul le système de caméras intelligentes permet l'affichage de l'affluence sur un tableau de bord en temps réel et l'envoi de notifications push.

---

<sup>15</sup> CJUE, *Huber*, C-524/06, ECLI:EU:C:2008:724, par. 59-61.

68. Le défendeur souligne que le même résultat ne pouvait pas être atteint en utilisant des systèmes de surveillance alternatifs, tels que des comptages manuels ou des mesures via des signaux Wi-Fi, étant donné que ces derniers ne sont pas suffisamment précis pour la finalité visée et que seul le système utilisé permet d'obtenir certaines informations supplémentaires nécessaires à la réalisation de cette finalité. Le défendeur affirme plus précisément que le respect ou non des règles de distanciation sociale, le sens de la circulation des passants et les différents types de passants - tels que les cyclistes et les piétons - ne peuvent être constatés par aucun système alternatif et que seul le système de caméras intelligentes permet un rapport en temps réel, ce qui est crucial pour pouvoir communiquer et, le cas échéant, intervenir en temps opportun.
69. En ce qui concerne la proportionnalité de l'activité de traitement concernée, le défendeur souligne que le traitement ne dure qu'une fraction de seconde, vu que les images des caméras filmées en direct sont quasi immédiatement anonymisées et transformées en *raw data* (données de comptage agrégées) et en images brouillées par le logiciel (en local sur la caméra même). Le défendeur insiste sur le fait que les images en direct ne sont ensuite stockées nulle part mais sont immédiatement supprimées de la mémoire de la caméra.
70. Le défendeur attire également l'attention sur le fait que le caractère proportionné de la mesure est également garanti par sa limitation dans le temps et dans l'espace. Il précise premièrement à cet égard que le contrat avec le sous-traitant a été délibérément conclu pour une courte période de trois mois et que la mesure n'a par conséquent été d'application que pendant cette période (à savoir la période estivale). Deuxièmement, il souligne le choix délibéré des lieux où ont été installées les caméras intelligentes en question et précise qu'il s'agissait uniquement des endroits où une affluence particulière était attendue (à savoir les digues et les rues commerçantes).
71. Sur la base de ce qui précède, la Chambre Contentieuse estime que le défendeur démontre la nécessité et la proportionnalité du système concerné en vue de la réalisation des finalités visées. Le défendeur démontre en effet l'absence d'un système alternatif - moins intrusif - qui pourrait réaliser ces finalités de la même façon. Il démontre également avoir pris les mesures nécessaires afin de garantir la proportionnalité (voir aussi ci-après).

**C. Protection des données dès la conception et protection des données par défaut (article 25 du RGPD)**

72. Lors du traitement de données à caractère personnel par des caméras (intelligentes), il est crucial - vu les risques potentiellement importants pour les droits et libertés des personnes

concernées - que le responsable du traitement prenne des mesures appropriées afin de veiller à ce que les principes en matière de protection des données soient intégrés de manière effective pour que les risques de violation des droits et libertés des personnes concernées soient limités autant que possible.

73. Les "mesures appropriées" susmentionnées ne sont pas de nature uniquement technique mais aussi organisationnelle et doivent être prises par le responsable du traitement *avant* le début des activités de traitement telles que, en l'espèce, la collecte d'images vidéos, à savoir au moment de déterminer les finalités et les moyens du traitement.<sup>16</sup>
74. En d'autres termes, le responsable du traitement doit respecter les principes de *'data protection by design'* (**protection des données dès la conception**) et de *'data protection by default'* (**protection des données par défaut**).<sup>17</sup>
75. Ces concepts constituent l'une des pierres angulaires du RGPD et du principe de responsabilité de l'article 5.2 *juncto* l'article 24 du RGPD, qui y occupe une position centrale. Ils sont repris à l'article 25 du RGPD et sont précisés au considérant 78 du RGPD.
76. Conformément à **l'article 25.1 du RGPD**, *"Compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, que présente le traitement pour les droits et libertés des personnes physiques, le responsable du traitement met en œuvre, tant au moment de la détermination des moyens du traitement qu'au moment du traitement lui-même, des mesures techniques et organisationnelles appropriées, telles que la pseudonymisation, qui sont destinées à mettre en œuvre les principes relatifs à la protection des données, par exemple la minimisation des données, de façon effective et à assortir le traitement des garanties nécessaires afin de répondre aux exigences du RGPD et de protéger les droits de la personne concernée"*.
77. **L'article 25.2 du RGPD** dispose que *"Le responsable du traitement met en œuvre les mesures techniques et organisationnelles appropriées pour garantir que, par défaut, seules les données à caractère personnel qui sont nécessaires au regard de chaque finalité spécifique du traitement sont traitées. Cela s'applique à la quantité de données à caractère personnel collectées, à l'étendue de leur traitement, à leur durée de conservation et à leur accessibilité. En particulier, ces mesures garantissent que, par défaut, les données à caractère personnel ne sont pas rendues accessibles à un nombre indéterminé de personnes physiques sans l'intervention de la personne physique concernée"*.

<sup>16</sup> Lignes directrices 3/2019, point 126.

<sup>17</sup> La Chambre Contentieuse utilisera ci-après l'abréviation "DPbDD" lorsqu'il s'agit simultanément des deux concepts.

78. **Le considérant 78 du RGPD** précise en ce qui concerne les mesures techniques et organisationnelles susmentionnées qu'elles "*pourraient consister, entre autres, à réduire à un minimum le traitement des données à caractère personnel, à pseudonymiser les données à caractère personnel dès que possible, à garantir la transparence en ce qui concerne les fonctions et le traitement des données à caractère personnel, à permettre à la personne concernée de contrôler le traitement des données, à permettre au responsable du traitement de mettre en place des dispositifs de sécurité ou de les améliorer*".
79. Dans ses Lignes directrices 4/2019 relatives à la DPbDD, l'EDPB précise que la protection des données par défaut renvoie à une valeur préexistante ou préétablie d'un paramètre ajustable au sein d'une application logicielle. Dans ces Lignes directrices, l'EDPB décrit la protection des données dès la conception comme ayant pour objectif de "*protéger les droits des personnes concernées et d'assurer que la protection de leurs données à caractère personnel soit propre ('intégrée') au traitement*".<sup>18</sup>
80. Dans sa jurisprudence, la Cour de justice a également souligné l'importance de ces concepts et a notamment affirmé dans son arrêt *Digital Rights Ireland* que l'essence de l'article 8 de la Charte des droits fondamentaux de l'Union européenne exige l'adoption de mesures techniques et organisationnelles afin de garantir que les données à caractère personnel sont efficacement protégées contre tout risque d'abus ainsi que contre tout accès et toute utilisation illicites de ces données.<sup>19</sup>
81. En l'espèce, la Chambre Contentieuse constate, sur la base tant des pièces du dossier que de la démonstration du système de caméras intelligentes par le défendeur lors de l'audition, que ce dernier a pris une série de mesures organisationnelles et techniques afin de limiter au maximum le traitement des données à caractère personnel d'une part et de protéger et sécuriser ces données d'autre part.
82. Ces mesures ont été prises après l'avis du délégué à la protection des données et après l'exécution d'une analyse d'impact relative à la protection des données sur la base de l'article 35 du RGPD par le défendeur en ce qui concerne le système de caméras intelligentes (voir également les points 131 e.s.).
83. La Chambre Contentieuse constate également que le défendeur a intégré la protection des données à caractère personnel *ab initio* dans la mise en œuvre du projet. Cela ressort

---

<sup>18</sup> EDBP, *Lignes directrices 4/2019 (version 2.0) sur la protection des données par conception et par défaut de l'article 25 du RGPD*, disponibles à l'adresse : [https://edpb.europa.eu/sites/edpb/files/consultation/edpb\\_guidelines\\_201904\\_dataprotection\\_by\\_design\\_and\\_by\\_default.pdf](https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_201904_dataprotection_by_design_and_by_default.pdf) (ci-après : Lignes directrices 4/2019).

<sup>19</sup> CJCE, affaires jointes C-293/12 et C-594/12, *Digital Rights Ireland*, par. 40 et 66-67.

notamment du fait que dans le cahier spécial des charges intitulé *"Comptage des passants à des endroits spécifiques sur la digue et dans des zones commerçantes à la Côte"* par lequel ce dernier a émis le marché public pour la mise en œuvre du système susmentionné, les dispositions contractuelles comportaient un titre concernant le traitement des données et le respect des dispositions du RGPD par le soumissionnaire, qui intervient comme sous-traitant des données. Lors de l'audition, le défendeur a précisé que le soumissionnaire final a notamment été sélectionné en raison de l'attention particulière qu'il portait à la protection des données à caractère personnel. Le défendeur agit ainsi conformément au prescrit du considérant 78 du RGPD, *in fine*, qui énonce à ce sujet que *"Les principes de protection des données dès la conception et de protection des données par défaut devraient également être pris en considération dans le cadre des marchés publics"*.

84. Il ressort des pièces du dossier ainsi que de la défense orale du défendeur que lors de la mise en œuvre proprement dite du système par le défendeur et le sous-traitant, une série de mesures techniques et organisationnelles ont également été prises en vue de la protection des données à caractère personnel, conformément aux articles 25.1 et 25.2 du RGPD.
85. Le premier article cité mentionne parmi ces mesures techniques et organisationnelles devant être prises par le responsable du traitement tout d'abord la pseudonymisation des données à caractère personnel en question. Le considérant 78 du RGPD mentionne également que *"Ces mesures pourraient consister, entre autres, [...] à pseudonymiser les données à caractère personnel dès que possible"*.
86. D'après les pièces du dossier et la démonstration du système de caméras intelligentes effectuée par le défendeur à la Chambre Contentieuse lors de l'audition, la Chambre Contentieuse comprend que le système de comptage des passants en question comporte un composant software et un composant hardware, associant à chaque caméra installée un *printed circuit board* ("PCB") fonctionnant comme un *Single Board Computer* local afin de traiter en local les images en temps réel. Les images des caméras (frames) sont traitées en local, sur place (*"on premise"*), par le PCB.
87. La démonstration du système lors de l'audition montre que les caméras en question filment bel et bien les passants, mais qu'en une fraction de seconde, les objets pertinents (comme les vélos et les voitures) ainsi que les personnes individuelles sont distingués et remplacés par ce que l'on appelle un "blob". Il s'agit d'une case colorée qui représente un passant ou un objet reconnu. Les passants filmés sont donc analysés en temps réel par l'intelligence artificielle et un algorithme d'auto-apprentissage.

88. Dans ses Lignes directrices 3/2019, l'EDPB a également souligné à cet égard que, appliqués au traitement de données à caractère personnel au moyen de dispositifs vidéos, des exemples de telles technologies respectueuses de la vie privée au sens de l'article 25 du RGPD sont les systèmes qui permettent de masquer ou de brouiller les zones non pertinentes ou de supprimer les images représentant des tiers dans le cadre de la transmission de séquences vidéo aux personnes concernées.<sup>20</sup>

89. Le défendeur explique à ce propos - notamment à l'aide de captures d'écran des caméras en question - que dans une première phase, à savoir pendant la première heure qui suit l'installation de ces caméras, on filme à basse résolution (image 1) et qu'ensuite, dans une seconde phase, les usagers sont remplacés par les "blobs" (également appelés "images brouillées" dans la présente décision). Le défendeur précise que le (bref) traitement de ces images s'effectue uniquement en local - plus précisément sur la caméra installée même - et qu'ensuite, deux flux de données partent de ces dispositifs vers le data center du sous-traitant, à savoir (i) les images brouillées et (ii) les données de comptage agrégées. Ces dernières données permettent de mesurer l'affluence - et de contrôler les règles de distanciation sociale - et d'intervenir au besoin. D'après les pièces du dossier et les explications fournies par le défendeur, les images des caméras proprement dites ne sont conservées nulle part.



*Figure 1. Images en basse résolution affichées par le firmware (phase 1)*

<sup>20</sup> Lignes directrices 3/2019, point 129.



Figure 2. Usagers remplacés par des "blobs" (phase 2)

90. Sur la base de ce qui précède, il apparaît que les images des caméras en question sont presque immédiatement anonymisées et que l'identification des passants filmés est rendue impossible.
91. La Chambre Contentieuse estime que ceci répond aux exigences de l'article 25.1 du RGPD et du considérant 78 du RGPD ainsi qu'au principe de minimisation des données repris à l'article 5.1 c) du RGPD, auquel il est également fait référence par les premières dispositions citées. Alors que l'article 25.1 du RGPD exige uniquement la pseudonymisation, les données à caractère personnel en question sont anonymisées de façon irréversible.
92. Grâce à cette anonymisation quasiment immédiate, seules sont en effet traitées les données à caractère personnel qui sont "*pertinentes*" et "*limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées*" et celles-ci sont ensuite converties en données de comptage anonymes ainsi qu'en images brouillées.
93. Les mesures décrites ci-dessus permettent également de répondre à l'exigence de l'article 25.2 du RGPD selon laquelle le responsable du traitement doit garantir que "*par défaut, seules les données à caractère personnel qui sont nécessaires au regard de chaque finalité spécifique du traitement sont traitées*", ce qui s'applique à "*la quantité de données à caractère personnel collectées, à l'étendue de leur traitement, à leur durée de conservation (...)*". Tant la quantité de données à caractère personnel que le délai de conservation des images en direct - qui est de seulement quelques millisecondes - sont ainsi limités au minimum, ce qui permet de respecter le principe de limitation de la conservation (art. 5.1 e) du RGPD.
94. Il ressort des pièces du dossier que le défendeur a également pris plusieurs autres mesures techniques et organisationnelles afin de limiter au maximum le traitement de données à caractère personnel, plus précisément :

- i. la limitation de la mesure dans l'espace, à savoir le placement de caméras intelligentes uniquement aux endroits présentant un risque de forte affluence (par exemple les digues et les zones commerçantes) ;
- ii. la limitation de la mesure dans le temps : le système de comptage des passants au moyen de caméras intelligentes a été utilisé de juin 2020 jusqu'au 30 septembre 2020, et ce à l'exception d'une seule commune, où en raison de l'affluence constante, l'utilisation du système a été prolongée jusqu'au 1<sup>er</sup> février 2021 ; et
- iii. la limitation et la sécurisation de l'accès aux images des caméras (voir ci-après).

95. L'article 25.2 *in fine* du RGPD dispose en ce qui concerne ce dernier aspect que l'accessibilité des données à caractère personnel en question doit être limitée, notamment pour garantir que *"par défaut, les données à caractère personnel ne [soient] pas rendues accessibles à un nombre indéterminé de personnes physiques sans l'intervention de la personne physique concernée"*.

96. La Chambre Contentieuse se réfère également à cet égard aux Lignes directrices 3/2019 de l'EDPB dans lesquelles ce dernier souligne l'importance en la matière de la sécurité du système et des données et déclare que cela fait référence à *"la sécurité physique de l'ensemble des composantes du système et à l'intégrité de celui-ci, c'est-à-dire la protection et la résilience contre toute ingérence, intentionnelle ou non, dans son fonctionnement normal et le contrôle d'accès"* ainsi qu'à *"la confidentialité (les données ne sont accessibles qu'aux personnes disposant d'un droit d'accès), à l'intégrité (la prévention contre la perte ou la manipulation des données) et à la disponibilité (les données sont rendues accessibles dès que cela est nécessaire)"*.<sup>21</sup>

97. À ce propos, la Chambre Contentieuse constate sur la base des pièces du dossier que le responsable du traitement ainsi que le sous-traitant ont pris les mesures techniques et organisationnelles nécessaires pour garantir la sécurité des données et limiter l'accès à celles-ci exclusivement aux personnes habilitées.

98. Dans ses conclusions en réponse, le défendeur précise plus spécifiquement à ce sujet que seul un nombre limité de collaborateurs (à savoir sept) du sous-traitant ont accès aux images en direct brouillées (et donc en principe anonymes) qui sont transférées au data center du sous-traitant et ce dans le seul objectif de contrôler le bon fonctionnement du système (par exemple : contrôler si la lentille des caméras est propre et si les caméras sont bien positionnées).

---

<sup>21</sup> Lignes directrices 3/2019, point 132.

99. Le défendeur démontre en outre que l'accès à ces images est soumis à des mesures de sécurité strictes et fait l'objet d'un traçage. Pendant l'audition, le défendeur précise à ce sujet que les collaborateurs autorisés ont uniquement accès aux images depuis le data center, que plusieurs mots de passe sont nécessaires pour obtenir l'accès à ces images et que l'accès est limité à quinze minutes. Le défendeur a également souligné en la matière que ni les communes participantes, ni lui-même n'ont accès aux images en direct des caméras. Il a ajouté n'avoir lui-même vu ces images (brouillées) pour la première fois qu'en préparation de l'audition dans le cadre de la présente procédure. Ces images en direct brouillées ne sont en outre stockées nulle part.
100. En ce qui concerne les mesures techniques et organisationnelles prescrites par l'article 25 du RGPD, l'EDPB souligne également dans ses Lignes directrices que les solutions choisies ne devraient pas offrir de fonctionnalités superflues (telles que des caméras à mouvement illimité ou disposant d'une capacité de zoom, de transmission radio ou d'analyse et d'enregistrement audio). L'EDPB ajoute à cela que les fonctions fournies mais qui ne sont pas nécessaires doivent être désactivées.<sup>22</sup>
101. Le défendeur précise à cet égard que dans le firmware du système concerné de caméras intelligentes, les fonctions qui ne sont pas nécessaires pour la finalité poursuivie ont été désactivées. Il précise encore qu'il a par exemple été rendu impossible de désactiver le brouillage appliqué. Le défendeur ajoute que le logiciel d'intelligence artificielle ne permet pas techniquement d'obtenir des images en direct non brouillées des caméras intelligentes et il se réfère à cet égard à une déclaration écrite du sous-traitant en la matière.
102. La Chambre Contentieuse attire l'attention sur l'importance essentielle des mesures techniques susmentionnées afin de garantir que les images ne puissent pas être utilisées de manière incompatible pour d'autres finalités que celles pour lesquelles les données ont été collectées (par exemple rendre les données accessibles à des tiers tels que les forces de l'ordre), ce qui serait contraire au principe de limitation des finalités repris à l'article 5.1 b) du RGPD.
103. Sur la base de ce qui précède, la Chambre Contentieuse conclut que, conformément à la responsabilité qui lui incombe en vertu de l'article 5.2 *juncto* l'article 24 du RGPD, le défendeur démontre que dès un stade précoce du projet des activités de traitement par le biais de l'utilisation du système de caméras intelligentes, il a pris les mesures techniques et organisationnelles appropriées nécessaires pour garantir d'emblée le respect des principes en

---

<sup>22</sup> Lignes directrices 3/2019, point 129.

matière de protection de la vie privée et des données. Le système mis en place par le défendeur constitue donc un bon exemple de "*data protection by design*" ("protection des données dès la conception") au sens de l'article 25 du RGPD.

104. Le défendeur démontre notamment que dès l'émission du marché public relatif au système de comptage des passants, il a tenu compte du respect des principes susmentionnés en prenant en considération des technologies qui répondent aux exigences de la DPbDD. Il a ainsi opté pour un système '*stand alone*', non connecté à un quelconque réseau, où le traitement de données à caractère personnel au moyen d'un dispositif vidéo est limité au minimum et où aucune autre donnée à caractère personnel n'est collectée.

105. Le défendeur a prévu un cadre de gestion approprié et a pris des mesures techniques concernant le traitement (envisagé), plus précisément en ce qui concerne :

- i. l'anonymisation, conformément à l'article 25.1 du RGPD et au considérant 78 du RGPD, grâce au "brouillage" automatique et irréversible des images des caméras après quelques millisecondes en remplaçant les piétons par des "blobs" ;
- ii. la minimisation des données (art. 5.1 c) du RGPD, grâce au délai de conservation court et à la limitation de la mesure dans le temps et dans l'espace ;
- iii. la limitation de la conservation, en ne conservant pas les images des caméras plus longtemps que ce qui est strictement nécessaire à la réalisation des finalités visées (enregistrement local pendant seulement quelques millisecondes) et en conservant les données obtenues sous une forme rendant impossible toute réidentification des personnes concernées, conformément à l'article 5.1 e) du RGPD ;
- iv. la sécurité des données et la limitation de l'accès, en limitant l'accès aux images en direct brouillées à un nombre limité de collaborateurs du sous-traitant habilités à cet effet (même lorsque les personnes sur ces images en direct brouillées ne peuvent en principe pas être réidentifiées), la sécurité de l'accès au système grâce à plusieurs mots de passe ainsi qu'au traçage de l'accès et également sa limitation dans le temps ;
- v. la désactivation des fonctionnalités superflues dans le firmware du système de manière à ce qu'aucune image en direct non brouillée qui permettrait l'identification des personnes concernées ne puisse être extraite des caméras et à ce qu'il soit techniquement impossible de désactiver le brouillage automatique des images.

106. Le défendeur a ainsi répondu aux exigences de l'article 25 du RGPD. La Chambre Contentieuse tient compte du fait que la crise sanitaire actuelle nécessite l'adoption de mesures exceptionnelles qui peuvent nécessiter le traitement de données à caractère personnel dans l'intérêt général, comme, par exemple, le fait de filmer des mouvements de

personnes. Dans ce contexte, il est essentiel qu'un responsable du traitement prenne le maximum de précautions pour limiter à un minimum les conséquences préjudiciables potentielles pour les personnes concernées dont les données sont traitées.

107. Sur la base de ce qui précède, la Chambre Contentieuse conclut également que le défendeur n'a pas enfreint les articles 5.1 a), 5.1 b) et 5.1 c) du RGPD et que ce dernier a suffisamment démontré avoir respecté les principes de protection des données lors du déploiement du système de comptage des passants.

*2.3.2. Transparence des informations et des communications et modalités de l'exercice des droits de la personne concernée (articles 12 et 13 du RGPD)*

108. Dans son rapport d'enquête, le Service d'Inspection constate que la déclaration de confidentialité du défendeur sur le site Internet [www.westtoer.be/nl/dataverwerking](http://www.westtoer.be/nl/dataverwerking)<sup>23</sup> ne répond pas aux obligations de transparence des articles 12.1, 12.6, 13.1 et 13.2 du RGPD.

109. Le Service d'Inspection constate tout d'abord à cet égard une violation des articles 12.1 et 12.6 du RGPD, notamment vu le fait que :

- 1) les informations qui sont fournies aux personnes concernées via la déclaration de confidentialité ne sont pas totalement correctes et ne sont donc pas transparentes, vu que l'on ne mentionne pas quelles modifications ont été apportées à cette déclaration de confidentialité ni à quel moment ;
- 2) le motif de licéité sur la base duquel le défendeur traite les données à caractère personnel des personnes concernées n'est pas mentionné de manière transparente ;
- 3) la déclaration de confidentialité indique à tort que les données à caractère personnel traitées à des fins d'étude statistique sont *pseudonymisées*, ce qui signifierait selon le défendeur que les données ne peuvent pas être reliées à un individu ;
- 4) la déclaration de confidentialité du défendeur indique à tort qu'une personne concernée qui souhaite exercer ses droits doit d'abord contacter le responsable du traitement et attendre sa réponse avant d'adresser sa demande au délégué à la protection des données;
- 5) la déclaration de confidentialité mentionne que pour l'exercice des droits des personnes concernées, une copie de la carte d'identité est demandée par le défendeur, ce qui serait disproportionné ; et que
- 6) en ce qui concerne la possibilité pour les personnes concernées d'introduire une plainte auprès d'une autorité de contrôle, la déclaration de confidentialité renvoie uniquement à

---

<sup>23</sup> Dont des captures d'écran ont été prises par le Service d'Inspection le 13 juillet 2020 ainsi que le 18 juillet 2020.

l'Autorité belge de protection des données, alors que l'article 77.1 du RGPD prévoit qu'une plainte peut être introduite auprès de n'importe quelle autorité de contrôle européenne.

110. Par ailleurs, le Service d'Inspection constate une violation des articles 13.1 et 13.2 du RGPD, vu que :

- 1) les finalités précises et la base juridique du traitement ne sont pas mentionnées dans la déclaration de confidentialité ;
- 2) les délais de conservation ou les critères utilisés pour déterminer ces délais ne sont pas mentionnés ; et que
- 3) le droit pour les personnes concernées de retirer le consentement donné pour l'utilisation de cookies n'est pas mentionné.

111. Lors de l'audition, le défendeur reconnaît que la déclaration de confidentialité a été adaptée tardivement mais il précise s'être avant tout concentré sur l'analyse d'impact relative à la protection des données ainsi que sur la licéité du système proprement dit. Le défendeur ajoute à cela que la déclaration de confidentialité a entre-temps été adaptée, suite et conformément aux constatations du Service d'Inspection, et il souligne qu'un conseiller juridique a été désigné afin d'adapter encore davantage, au besoin, les documents relatifs à la protection de la vie privée à partir de la mi-janvier 2021.

112. La Chambre Contentieuse attire l'attention sur le fait que conformément à l'article 12.1 du RGPD, le responsable du traitement *"[prend] des mesures appropriées pour fournir toute information visée aux articles 13 et 14 ainsi que pour procéder à toute communication au titre des articles 15 à 22 et de l'article 34 en ce qui concerne le traitement à la personne concernée d'une façon concise, transparente, compréhensible et aisément accessible, en des termes clairs et simples (...)"*.

113. Les considérants 58 et 60 du RGPD précisent que *"Le principe de traitement loyal et transparent exige que la personne concernée soit informée de l'existence de l'opération de traitement et de ses finalités"* et que *"Le principe de transparence exige que toute information adressée au public ou à la personne concernée soit concise, aisément accessible et facile à comprendre (...)"*.

114. Dans le cas où les données à caractère personnel en question n'ont pas été collectées auprès de la personne concernée elle-même, l'article 13 du RGPD prescrit quelles informations doivent être fournies à cette dernière :

*“Lorsque des données à caractère personnel relatives à une personne concernée sont collectées auprès de cette personne, le responsable du traitement lui fournit, au moment où les données en question sont obtenues, toutes les informations suivantes :*

- a) l'identité et les coordonnées du responsable du traitement et, le cas échéant, du représentant du responsable du traitement ;*
- b) le cas échéant, les coordonnées du délégué à la protection des données ;*
- c) les finalités du traitement auquel sont destinées les données à caractère personnel ainsi que la base juridique du traitement ;*
- d) lorsque le traitement est fondé sur l'article 6, paragraphe 1, point f), les intérêts légitimes poursuivis par le responsable du traitement ou par un tiers ; e) les destinataires ou les catégories de destinataires des données à caractère personnel, s'ils existent; et*
- f) le cas échéant, le fait que le responsable du traitement a l'intention d'effectuer un transfert de données à caractère personnel vers un pays tiers ou à une organisation internationale, et l'existence ou l'absence d'une décision d'adéquation rendue par la Commission ou, dans le cas des transferts visés à l'article 46 ou 47, ou à l'article 49, paragraphe 1, deuxième alinéa, la référence aux garanties appropriées ou adaptées et les moyens d'en obtenir une copie ou l'endroit où elles ont été mises à disposition.*

*2. En plus des informations visées au paragraphe 1, le responsable du traitement fournit à la personne concernée, au moment où les données à caractère personnel sont obtenues, les informations complémentaires suivantes qui sont nécessaires pour garantir un traitement équitable et transparent :*

- a) la durée de conservation des données à caractère personnel ou, lorsque ce n'est pas possible, les critères utilisés pour déterminer cette durée ;*
- b) l'existence du droit de demander au responsable du traitement l'accès aux données à caractère personnel, la rectification ou l'effacement de celles-ci, ou une limitation du traitement relatif à la personne concernée, ou du droit de s'opposer au traitement et du droit à la portabilité des données ;*
- c) lorsque le traitement est fondé sur l'article 6, paragraphe 1, point a), ou sur l'article 9, paragraphe 2, point a), l'existence du droit de retirer son consentement à tout moment, sans porter atteinte à la licéité du traitement fondé sur le consentement effectué avant le retrait de celui-ci ; d) le droit d'introduire une réclamation auprès d'une autorité de contrôle ;*
- e) des informations sur la question de savoir si l'exigence de fourniture de données à caractère personnel a un caractère réglementaire ou contractuel ou si elle conditionne la conclusion d'un contrat et si la personne concernée est tenue de fournir les données à caractère personnel, ainsi que sur les conséquences éventuelles de la non-fourniture de ces données ;*
- f) l'existence d'une prise de décision automatisée, y compris un profilage, visée à l'article 22, paragraphes 1 et 4, et, au moins en pareils cas, des informations utiles concernant la logique*

*sous-jacente, ainsi que l'importance et les conséquences prévues de ce traitement pour la personne concernée*'.

115. La Chambre Contentieuse a consulté la déclaration de confidentialité du défendeur (dernière consultation le 05/02/2021) et a en effet constaté à cette occasion que celle-ci a effectivement été adaptée de manière à tenir compte de la majorité des remarques du Service d'inspection et que par conséquent, la déclaration de confidentialité a été presque entièrement mise en conformité avec les dispositions afférentes du RGPD. La Chambre Contentieuse en prend acte.

116. L'on observe toutefois que toutes les constatations du Service d'Inspection n'ont pas encore été prises en compte.

117. La Chambre Contentieuse constate tout d'abord à cet égard que la déclaration de confidentialité ne mentionne pas de façon suffisamment détaillée le(s) fondement(s) juridique(s) du traitement des données à caractère personnel en question, comme le requiert l'article 13.1 c) du RGPD. La déclaration de confidentialité mentionne notamment à cet égard :

*"Nous traitons vos données à caractère personnel sur la base soit :*

- *de votre consentement.*
- *d'un contrat passé entre nous.*
- *d'une obligation légale à laquelle nous devons satisfaire.*
- *d'un intérêt public."*

118. Il n'est toutefois pas précisé de quelles obligations légale ou de quel intérêt public il s'agit. Ainsi, par exemple pour le traitement des données à caractère personnel via le système de caméras intelligentes, il n'est pas mentionné spécifiquement quel est le fondement légal pour le traitement en question (voir ci-avant l'article 6.3 du RGPD).

119. Conformément aux Lignes directrices sur la transparence rédigées par le Groupe 29, les informations fournies sur la base des articles 13 et/ou 14 du RGPD doivent être concrètes et définitives et ne peuvent comporter aucune formule abstraite ou ambiguë. Le Groupe 29 souligne que cela vaut particulièrement pour les finalités et le fondement juridique du traitement.<sup>24</sup>

---

<sup>24</sup> Lignes directrices sur la transparence au sens du Règlement (UE) 2016/679, WP260rev01, établies le 29 novembre 2017, p. 9-10.

120. La Chambre Contentieuse estime que cela constitue une violation de l'article 13.1 c) du RGPD et recommande dès lors au défendeur de préciser ce(s) fondement(s) juridique(s) conformément à la disposition susmentionnée.

121. Deuxièmement, la Chambre Contentieuse constate que la déclaration de confidentialité ne mentionne pas non plus clairement les délais de conservation des données à caractère personnel concernés ou les critères permettant de les déterminer, comme le requiert l'article 13.2 a) du RGPD. La déclaration de confidentialité mentionne à ce sujet que *"les données sont conservées aussi longtemps que nécessaire pour pouvoir offrir nos services, parce que nous avons un intérêt à le faire ou pour remplir nos obligations légales"*. Il ressort toutefois des Lignes directrices du Groupe 29 qu'une telle formulation est insuffisante. Le Groupe 29 souligne à cet égard que le délai / la mention du délai de conservation est lié(e) au principe de minimisation des données repris à l'article 5.1, c) du RGPD ainsi qu'à l'exigence de limitation de conservation édictée à l'article 5.1, e) du RGPD. Il précise que *"La période de conservation (ou les critères pour la déterminer) peut être dictée par différents facteurs comme des exigences réglementaires ou des lignes directrices industrielles, mais elle devrait être formulée de manière à ce que la personne concernée puisse évaluer, selon la situation dans laquelle elle se trouve, quelle sera la période de conservation s'agissant de données spécifiques ou en cas de finalités spécifiques."*<sup>25</sup>

122. La Chambre Contentieuse recommande par conséquent au défendeur de préciser davantage les délais de conservation des données à caractère personnel collectées dans la déclaration de confidentialité, conformément à l'article 13.2 a) du RGPD.

123. La Chambre Contentieuse constate en outre que la déclaration de confidentialité mentionne ce qui suit concernant l'exercice des droits des personnes concernées :

*"Il se peut que nous ayons besoin d'une preuve de votre identité pour pouvoir répondre à votre demande. Dans ce cas, nous vous demanderons de fournir une copie ou un scan de votre carte d'identité ou de tout autre justificatif de votre identité. Nous utiliserons cette preuve uniquement pour établir que vous êtes effectivement la personne concernée dont les données à caractère personnel sont traitées, ou bien le parent ou le tuteur pour les moins de 16 ans. Dès que nous serons tous deux satisfaits de la réponse à votre question, nous détruirons cette preuve"*.

124. Comme également relevé par le Service d'Inspection, la Chambre Contentieuse souligne que conformément à l'article 12.6 du RGPD, le responsable du traitement peut uniquement demander des informations supplémentaires à la personne concernée *"[lorsqu'il] a des*

---

<sup>25</sup> Groupe 29, Lignes directrices sur la transparence au sens du Règlement (UE) 2016/679, WP260Rev1, p. 45.

*doutes raisonnables quant à l'identité de la personne physique présentant la demande visée aux articles 15 à 21*". La réclamation systématique d'une copie ou d'un scan de la carte d'identité de la personne concernée est par conséquent disproportionnée.

125. La Chambre Contentieuse souligne à cet égard que ce n'est que dans les cas spécifiques où conformément à l'article 5.2 du RGPD, le responsable du traitement est à même de démontrer qu'il ne peut pas identifier cette personne concernée (art. 11.2 du RGPD) et/ou qu'il a des doutes raisonnables quant à l'identité de la personne physique présentant la demande (art. 12.6 du RGPD) qu'il peut réclamer les données supplémentaires nécessaires pour confirmer l'identité de la personne concernée. Ces données supplémentaires peuvent par exemple consister en une copie du recto de la carte d'identité où ne sont lisibles que les données à caractère personnel qui sont strictement nécessaires pour cette vérification. Les autres données peuvent avoir été préalablement rendues illisibles par le plaignant.

126. La Chambre Contentieuse constate que les autres constatations du Service d'Inspection ont entre-temps été prises en considération par les modifications apportées par le défendeur à la déclaration de confidentialité, mais elle constate cependant qu'elles étaient établies à l'époque où l'enquête d'inspection a été effectuée.

127. Le défendeur le reconnaît et souligne dans sa défense, comme mentionné ci-avant, qu'il s'est avant tout concentré sur la conformité au RGPD du système des caméras intelligentes proprement dit avant d'adapter la déclaration de confidentialité.

128. La Chambre Contentieuse souligne toutefois l'importance du respect des obligations de transparence dans le chef d'un responsable du traitement dès le début de l'activité de traitement, vu l'impact que cela a sur l'exercice des droits des personnes concernées énoncés aux articles 15 à 22 inclus du RGPD, comme l'illustre la jurisprudence de la Cour de justice.<sup>26</sup>

129. La Chambre Contentieuse souligne en outre qu'en tant que régie provinciale autonome chargée d'une tâche d'intérêt public, le défendeur a un rôle d'exemple au niveau du respect de la législation relative à la protection des données à caractère personnel et que par conséquent, conformément *au principe du "lead by example"*, il doit veiller en tout temps à agir conformément à cette législation et en particulier à se conformer aux dispositions essentielles susmentionnées du RGPD concernant la transparence.<sup>27</sup>

---

<sup>26</sup> CJUE, 1<sup>er</sup> octobre 2015, *Bara*, C-201/14, ECLI:EU:C:2015:638.

<sup>27</sup> Autorité de protection des données, *Plan Stratégique 2020-2025*, [https://www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents/APD\\_Plan\\_Strategique\\_28012020.pdf](https://www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents/APD_Plan_Strategique_28012020.pdf), p. 22.

130. Vu la coopération du défendeur et l'adaptation de la déclaration de confidentialité au cours de la procédure, la Chambre Contentieuse ne juge toutefois pas nécessaire d'assortir les constatations susmentionnées d'une sanction, mais elle ordonne néanmoins au défendeur de mettre cette déclaration de confidentialité entièrement en conformité.

*2.3.3. L'analyse d'impact relative à la protection des données (articles 35.2 et 35.7 du RGPD)*

131. Selon le Service d'Inspection, le défendeur a commis une violation des articles 35.2 et 35.7 du RGPD. Le Service d'Inspection estime que le défendeur n'as pas recueilli, ou en tout cas pas à temps, l'avis du délégué à la protection des données sur une AIPD (article 35.2). Le Service d'Inspection considère en outre que le défendeur n'as pas respecté l'article 35.7 du RGPD, qui prescrit que l'AIPD doit contenir les éléments suivants : a) une description systématique des opérations de traitement envisagées et des finalités du traitement, y compris, le cas échéant, l'intérêt légitime poursuivi par le responsable du traitement ; b) une évaluation de la nécessité et de la proportionnalité des opérations de traitement au regard des finalités ; c) une évaluation des risques pour les droits et libertés des personnes concernées ; d) les mesures envisagées pour faire face aux risques, y compris les garanties, mesures et mécanismes de sécurité visant à assurer la protection des données à caractère personnel.

132. Le défendeur a fait savoir dans les réponses aux questions du Service d'Inspection que le délégué à la protection des données a été impliqué d'emblée dans la réalisation de l'AIPD concernant les caméras intelligentes. Selon le défendeur, la première concertation concernant l'AIPD a eu lieu le 11 juin 2020. Dans les conclusions, le défendeur répète que tant le délégué à la protection des données que le défendeur ont clairement indiqué que le délégué avait été présent et associé à la réalisation de l'AIPD dès le début le 11 juin 2020. Le Service d'Inspection estime par contre qu'il n'est pas démontré que la concertation susmentionnée a effectivement eu lieu et que le délégué à la protection des données y était présent. Dans l'avis du délégué à la protection des données, il est fait référence à l'AIPD avec les termes "l'AIPD élaborée".<sup>28</sup> Selon le Service d'Inspection, ce qui précède indique que l'AIPD (du moins une partie de celle-ci) avait déjà été rédigée avant que le délégué ne rende son avis. D'après le Service d'Inspection, il manque en outre une évaluation des risques visés à l'article 35.1 du RGPD pour les droits et libertés des personnes concernées (voir l'article 35.7 c) ainsi que les mesures envisagées pour faire face aux risques, y compris les garanties, mesures et mécanismes de sécurité visant à assurer la protection des données à caractère personnel (article 35.7 d).

---

<sup>28</sup> Avis sur l'AIPD du délégué à la protection des données annexe 5 par e-mail du 28 juillet 2020 du défendeur.

133. D'après la Chambre Contentieuse, les documents présentés ne permettent en effet pas d'établir qu'une discussion concernant l'élaboration d'une AIPD ait eu lieu le 11 juin 2020 en présence du délégué à la protection des données. En l'absence de preuve de la présence ou de l'absence du délégué, la Chambre Contentieuse ne peut pas se prononcer davantage à ce sujet.

134. Il ressort toutefois bel et bien des documents soumis que le délégué à la protection des données de Westtoer a transmis son avis écrit (daté du 17 juin 2020) à Westtoer en date du 18 juin 2020. Dans cet avis, des remarques sont formulées et le délégué à la protection des données a approuvé l'AIPD. Selon le Groupe 29, le responsable du traitement doit recueillir l'avis du délégué à la protection des données concernant une AIPD, notamment sur les questions suivantes :

- *quelle méthodologie faut-il suivre lors de la réalisation d'une analyse d'impact relative à la protection des données ;*
- *l'analyse d'impact relative à la protection des données doit-elle être effectuée en interne ou être externalisée ;*
- *quelles garanties (dont les mesures techniques et organisationnelles) doivent être appliquées afin d'atténuer les risques éventuels pesant sur les droits et les intérêts des personnes concernées ;*
- *la question de savoir si l'analyse d'impact relative à la protection des données a été correctement réalisée et si ses conclusions (opportunité ou non de procéder au traitement et garanties à mettre en place) sont conformes au RGPD.<sup>29</sup>*

135. La Chambre Contentieuse estime que dans l'avis écrit du 17 juin 2020 du délégué à la protection des données, on peut trouver une description des risques éventuels que le traitement de données pourrait entraîner ainsi qu'une description des garanties pouvant être appliquées pour les contrer. Le délégué à la protection des données a également indiqué dans l'avis que l'AIPD répondait aux exigences de l'article 35.7 du RGPD et y a souligné que l'AIPD tenait également compte des points d'attention décrits par le délégué dans son avis. Le 25 juin 2020, donc une semaine après l'avis écrit du délégué, l'AIPD a été approuvée et signée par le directeur général et le président du conseil d'administration du défendeur. Au vu de ce qui précède ainsi que des moyens et justificatifs invoqués, la Chambre Contentieuse estime donc, contrairement au Service d'Inspection, que le délégué à la protection des données a bel et bien rendu un avis sur l'AIPD. Aucune violation de l'article 35.2 du RGPD ne peut être constatée.

---

<sup>29</sup> Groupe 29 WP 243 rev.01

136. Selon le Service d'Inspection, il est en outre question de violations de l'article 35.7 c) et d) du RGPD. D'après le Service d'Inspection, l'AIPD contient une description trop sommaire des risques pour les droits et libertés des personnes concernées. L'AIPD ne montrerait pas comment l'évaluation des risques a été réalisée. Le Service d'Inspection considère que les mesures envisagées pour faire face aux risques, y compris les garanties, mesures et mécanismes de sécurité visant à assurer la protection des données à caractère personnel et à apporter la preuve du respect du RGPD ont été décrites trop brièvement et de façon insuffisante.

137. La Chambre Contentieuse estime que les risques que les traitements pourraient engendrer ont été décrits et évalués avec suffisamment de précision dans l'AIPD élaborée. Comme la Chambre Contentieuse l'a déjà constaté ci-avant dans la présente décision, le défendeur est parvenu à la fois sur la base d'une série de mesures techniques et organisationnelles ainsi qu'en limitant, protégeant et sécurisant autant que possible le traitement de données à caractère personnel, à prendre les mesures nécessaires contre d'éventuels risques. La Chambre Contentieuse considère donc qu'aucune violation de l'article 35.7 n'a été commise.

2.4. En ce qui concerne les constatations du Service d'Inspection *en dehors du cadre* des indices sérieux

*2.4.1. Le consentement au placement de cookies (articles 4.11, 6.1 a), 7.1 et 7.3 du RGPD)*

138. Le Service d'Inspection arrive à la conclusion que le défendeur ne demande pas de consentement pour le placement de cookies sur le site Internet <https://www.westtoer.be>. Le Service d'Inspection constate une violation des articles 4.11, 6.1 a) et 7.1 et 7.3 du RGPD. Les captures d'écran du site Internet susmentionné prises par le Service d'Inspection le 13 juillet 2019<sup>30</sup> montrent que les personnes concernées qui se rendent sur le site Internet de Westtoer étaient supposées avoir donné leur consentement au moment où elles poursuivent leur navigation sur le site. C'est la raison pour laquelle il n'était pas demandé au préalable aux personnes concernées de donner leur consentement pour l'utilisation de cookies sur le site Internet. Le consentement n'est pas non plus demandé pour le placement de cookies non essentiels. Cela ressort de la phrase "*En utilisant le présent site ou en cliquant sur 'Approuver', vous consentez à l'utilisation de cookies*".

---

<sup>30</sup> Pièce 8 du rapport d'Inspection du 25 août 2019

139. La notion de "consentement" est constituée de plusieurs éléments qui doivent être cumulativement respectés. L'article 4.11 du RGPD définit le consentement comme étant : *"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"*. L'élément "libre" doit être interprété comme le fait d'offrir effectivement un choix et de laisser le contrôle de ce choix à la personne concernée. Lorsqu'une personne concernée n'a pas eu effectivement le choix et qu'elle se sent contrainte de donner son consentement parce que les conséquences d'un refus seraient préjudiciables, le consentement est réputé ne pas avoir été donné librement. Si le consentement constitue une partie non négociable des conditions, on considère qu'il n'a pas été donné librement. Ceci signifie que le consentement ne sera pas considéré comme avoir été donné librement si la personne concernée n'est pas en mesure de refuser ou de retirer son consentement sans subir de conséquences.<sup>31</sup>

140. La Chambre Contentieuse se réfère à cet égard<sup>32</sup> à l'arrêt *Planet 49* de la Cour de justice européenne.<sup>33</sup> Dans cet arrêt, la Cour de justice de l'Union européenne a précisé l'exigence de consentement pour le placement de cookies suite à l'entrée en vigueur du RGPD et a expliqué qu'un consentement actif explicite était désormais prescrit :

*"Un consentement actif est ainsi désormais expressément prévu par le règlement 2016/679. Il importe de relever à cet égard que, selon le considérant 32 de ce règlement, l'expression du consentement pourrait se faire notamment en cochant une case lors de la consultation d'un site Internet. Ledit considérant exclut en revanche expressément qu'il y ait un consentement "en cas de silence, de cases cochées par défaut ou d'inactivité". Il s'ensuit que le consentement visé à l'article 2, sous f), et à l'article 5, paragraphe 3, de la directive 2002/58, lus conjointement avec l'article 4, point 11, et l'article 6, paragraphe 1, sous a), du règlement 2016/679, n'est pas valablement donné lorsque le stockage d'informations ou l'accès à des informations déjà stockées dans l'équipement terminal de l'utilisateur d'un site Internet est autorisé par une case cochée par défaut que l'utilisateur doit décocher pour refuser de donner son consentement." (Soulignement de la Chambre Contentieuse)*

141. Comme décrit ci-dessus, le Service d'Inspection a constaté le 13 juillet 2019 que les visiteurs du site Internet étaient supposés avoir donné leur consentement à l'utilisation de cookies dès le moment où elles décident de poursuivre leur navigation sur le site. Il n'est pas question de

<sup>31</sup> Voir plus en détail les Lignes directrices 5/2020 de l'EDPB relatives au consentement.

<sup>32</sup> Voir également plus en détail la Décision 12/2019 de la Chambre Contentieuse.

<sup>33</sup> Arrêt CJUE du 1<sup>er</sup> octobre 2019, C-673/17, Planet49, ECLI:EU:C:2019:801.

consentement préalablement demandé. Il ressort toutefois de l'article 6.1 du RGPD que ce consentement doit être obtenu préalablement au traitement. En n'obtenant pas de consentement préalable des personnes concernées, le défendeur a agi en violation des articles 6.1 a) et 7.1 du RGPD.

142. Dans ses conclusions en réponse du 1<sup>er</sup> octobre 2020, le défendeur a reconnu que la politique en matière de cookies pouvait être améliorée. Lors de l'audition, le défendeur fait savoir qu'entre-temps, la politique en matière de cookies a été mise en conformité avec la législation en vigueur en matière de vie privée et que dorénavant, des cookies sont placés uniquement lorsqu'un consentement actif a été obtenu à cet effet. Le Service d'Inspection constate également que le défendeur ne respecte pas l'article 7.3 du RGPD dans lequel il est indiqué que la personne concernée doit avoir le droit de retirer son consentement à tout moment. Dans la première version de la politique en matière de cookies examinée par le Service d'Inspection le 13 juillet 2020, ce dernier constate qu'aucune information n'est donnée aux personnes concernées sur leur droit de retirer le consentement qu'elles donnent pour l'utilisation de cookies. La mention relative aux cookies qui était utilisée était la suivante<sup>34</sup> : "En utilisant le présent site ou en cliquant sur "Approuver", vous consentez à l'utilisation de cookies". Une option indiquant "OK, je suis d'accord" était également affichée. Hormis le bouton d'accord, aucune autre option n'était offerte ni la possibilité de retirer l'accord donné.

143. Dans ses conclusions en réponse, en ce qui concerne la possibilité de retrait du consentement pour les cookies, le défendeur déclare ce qui suit<sup>35</sup> :

*"Enfin, le Service d'Inspection déclare que les personnes concernées ne sont pas suffisamment informées à propos de leur droit de retirer leur consentement pour l'utilisation de cookies. C'est inexact. Tout d'abord, la déclaration de confidentialité indique de manière générale que "Pour certains traitements, vous avez le droit, en tant que personne concernée, de retirer votre consentement gratuitement à tout moment". Ce droit peut évidemment aussi être exercé lorsque le consentement a été donné pour les cookies. En outre, la déclaration de confidentialité mentionne spécifiquement pour les cookies la manière dont ces cookies peuvent être supprimés par les utilisateurs : "Les paramètres de votre navigateur vous permettent d'empêcher l'utilisation de cookies ou de recevoir certaines notifications lors de l'installation ou de la suppression de cookies . [...]"*

*En cliquant sur les liens des navigateurs susmentionnés, une explication détaillée est fournie sur la manière de supprimer les cookies (le lien vers Google Chrome affiche par ex. bien en*

---

<sup>34</sup> Capture d'écran du site Internet prise par le Service d'Inspection.

<sup>35</sup> Conclusions en réponse du défendeur, p. 19.

*évidence "Autoriser ou bloquer les cookies"). Dans la pratique, l'utilisateur peut donc décider à tout moment que les cookies ne peuvent plus être traités."*

144. La Chambre Contentieuse ne partage pas la position du défendeur et se rallie à cet égard à la constatation du Service d'Inspection selon laquelle dans la première version (du 13 juillet 2020) de la politique en matière de cookies, le défendeur n'a pas respecté les exigences de l'article 7.3 du RGPD, libellé comme suit : *"La personne concernée a le droit de retirer son consentement à tout moment. Le retrait du consentement ne compromet pas la licéité du traitement fondé sur le consentement effectué avant ce retrait. La personne concernée en est informée avant de donner son consentement. Il est aussi simple de retirer que de donner son consentement."*<sup>36</sup> D'après la Chambre Contentieuse, il est évident que retirer son consentement n'est pas aussi simple que de le donner. Outre le bouton permettant d'accepter la politique en matière de cookies, aucun choix n'était proposé pour retirer le consentement donné. Comme décrit au point 8, la personne concernée devait parcourir plusieurs étapes via les paramètres du navigateur avant que le consentement puisse être retiré. La Chambre Contentieuse constate dès lors une violation de l'article 7.3 du RGPD.

145. Le 6 décembre 2020, la Chambre Contentieuse a analysé le site Internet <https://www.westtoer.be> afin de vérifier si des modifications avaient été apportées dans la politique en matière de cookies du défendeur depuis l'enquête du Service d'Inspection, comme indiqué ci-dessus. C'était effectivement le cas. La Chambre Contentieuse constate que dans la fenêtre pour la gestion des cookies, une distinction est à présent établie entre les cookies suivants : *essentiels, fonctionnels, analytiques, publicitaires*. Le cookie "essentiel" est pré-coché et il n'est pas possible de le décocher. Les autres cookies - non essentiels - peuvent être cochés mais ils sont en principe décochés.

146. La politique en matière de cookies, dans sa forme actuelle, permet bien aux personnes concernées de retirer leur consentement aussi facilement que de le donner. En effet, la fenêtre pour la gestion des cookies mentionne ce qui suit : *"Voulez-vous profiter d'une expérience optimale ? Cliquez ci-dessous sur "Accepter" si vous acceptez l'utilisation de cookies pour toutes les finalités susmentionnées". Vous pouvez aussi paramétrer vos propres préférences. Vous pouvez à tout moment adapter à nouveau vos choix.*" À côté du bouton "Accepter", se trouve un bouton "adapter les préférences" grâce auquel un consentement donné peut facilement être retiré.

---

<sup>36</sup> Soulignement par la Chambre Contentieuse.

147. La Chambre Contentieuse prend acte de ce qui précède. Vu le fait que la politique en matière de cookies a entre-temps été adaptée, la Chambre Contentieuse se limite à infliger une réprimande pour les violations de l'article 6.1 a) et des articles 7.1 et 7.3 du RGPD constatées par le Service d'Inspection.

*2.4.2. Registre des activités de traitement (article 30 du RGPD)*

148. Aux termes de l'article 30.1. du RGPD, le responsable du traitement - et le cas échéant son représentant - doit tenir un registre des activités de traitement effectuées sous sa responsabilité.

Le Service d'Inspection est arrivé à la conclusion que le défendeur ne répond pas à l'article 30.1. D'après le Service d'Inspection : les coordonnées du responsable du traitement sont incomplètes et donc non conformes à l'article 30.1 a) (ceci car l'adresse e-mail [dataverwerking@westtoer.be](mailto:dataverwerking@westtoer.be) n'est pas mentionnée) ; la description des catégories de personnes concernées n'est pas complète (article 30.1 c)), car dans la colonne "catégories de personnes physiques", le mot "autres" est mentionné à plusieurs endroits ; les pays tiers auxquels les données à caractère personnel sont transmises ne sont pas renseignés (article 30.1 e)) et il y a plusieurs mentions d' "(adresses e-mail à Mailchimp)" sans que l'on sache clairement de quels pays il s'agit ; le registre ne mentionne nulle part le traitement de données à caractère personnel de visiteurs du site Internet via l'utilisation de cookies.

149. Le défendeur affirme dans ses conclusions que les coordonnées de Westtoer ne peuvent pas être qualifiées d'incomplètes uniquement en raison de l'absence de l'adresse e-mail [dataverwerking@westtoer.be](mailto:dataverwerking@westtoer.be). Selon le défendeur, l'article 30.1 a) du RGPD n'exige pas que chaque adresse e-mail du responsable du traitement soit mentionnée. Le registre comporte en effet les coordonnées à la fois de Westtoer et du délégué à la protection des données. Le défendeur estime que l'article 30.1 a) est ainsi respecté. Le défendeur estime également incorrect de considérer la description des catégories de personnes concernées comme étant incomplète en raison de l'utilisation du mot "autres". Le défendeur indique ainsi que : *"un menu déroulant permet de choisir les catégories suivantes : (i) employés, (ii) clients, (iii) fournisseurs, (iv) autres, (v) postulants, (vi) visiteurs du site Internet. La catégorie "autres" vise donc les personnes concernées qui ne sont pas des employés, des clients, des fournisseurs, des postulants ou des visiteurs du site Internet - comme par exemple les passants dans le système de comptage des passants. Compte tenu des remarques du Service d'Inspection, Westtoer adaptera le registre afin de désigner la catégorie "Autres" avec davantage de précision".*

150. La Chambre Contentieuse a pris connaissance du registre des activités de traitement et constate que les coordonnées tant du responsable du traitement que du délégué à la protection des données (telles qu'indiquées également par le défendeur) sont reprises. L'adresse e-mail [dateverwerking@westtoer.be](mailto:dateverwerking@westtoer.be) n'apparaît effectivement pas parmi ces données du responsable du traitement. Toutefois, les coordonnées du responsable du traitement ainsi que du délégué à la protection des données figurent dans le registre. La Chambre contentieuse estime que dans un souci d'exhaustivité et de bonne joignabilité, il est recommandé d'également reprendre l'adresse e-mail susmentionnée dans le registre. La constatation du Service d'Inspection selon laquelle la description des catégories de personnes concernées est incomplète en raison de l'utilisation du mot "autres" est correcte dans les faits. Toutefois, comme le défendeur l'a expliqué dans ses conclusions, le registre reprend différentes catégories dont la catégorie "autres" fait partie et qui est mentionnée à plusieurs reprises. Un clic sur "détails de l'activité de traitement" du registre des activités de traitement permet de déterminer quelle catégorie est visée par "autres". La Chambre Contentieuse estime que sur ce point des catégories (article 30.1 c)), le registre n'est pas contraire au RGPD, mais elle recommande au défendeur d'expliquer dorénavant aussi la catégorie "autres".

151. La Chambre Contentieuse constate que la description des pays tiers auxquels les données à caractère personnel sont transmises manque de clarté. Dans le registre des activités de traitement, sous l'onglet transfert de données à caractère personnel à des pays tiers, il est mentionné "oui (*adresses e-mail à Mailchimp*)" avec à côté un lien supplémentaire. En cliquant sur le lien indiqué, on arrive sur la politique de confidentialité de Mailchimp qui indique dans quel pays cette organisation est établie. Dans ses conclusions, le défendeur a signalé que le fait de reprendre le lien vers la politique de confidentialité de Mailchimp indique que des transferts de données à caractère personnel peuvent avoir lieu vers les États-Unis. La Chambre Contentieuse estime important d'indiquer désormais explicitement et de manière univoque dans le registre des activités de traitement vers quels pays les données à caractère personnel sont transférées.

152. Vu ce qui précède, la Chambre Contentieuse estime que le registre des activités de traitement n'est pas conforme sur ce point, ce qui permet de constater une violation de l'article 30 du RGPD. Cette violation n'est pas de nature à nécessiter une sanction.

#### *2.4.3. Le délégué à la protection des données (article 37 et 38 du RGPD)*

153. Conformément à l'article 37.5 du RGPD, le délégué à la protection des données est désigné sur la base de ses qualités professionnelles et, en particulier, de ses connaissances

spécialisées du droit et des pratiques en matière de protection des données. De l'avis de la Chambre Contentieuse, les documents que le défendeur a fait parvenir au Service d'Inspection attestent de manière suffisante que le niveau de formation et l'expérience pratique du délégué à la protection des données répondent à l'exigence énoncée dans l'article susmentionné<sup>37</sup>. Le défendeur respecte également l'article 37.7 du RGPD puisque les données à caractère personnel du délégué à la protection des données ont été communiquées par le défendeur à l'Autorité de protection des données.

154. L'article 38.2 du RGPD dispose que le responsable du traitement aide le délégué à la protection des données dans ses missions en lui fournissant accès aux données à caractère personnel et en mettant à sa disposition les ressources nécessaires pour exercer ces missions. D'après le Service d'Inspection, une violation de l'article 38.2 du RGPD est établie vu qu'il ne ressort pas des réponses du défendeur à combien d'agences le délégué à la protection des données émet un avis et quelles sont ces agences. Le défendeur réagit comme suit à la constatation du Service d'Inspection : *"Nous ne savons pas ce que le Service d'Inspection reproche exactement à Westtoer, mais il semble que le Service d'Inspection affirme que l'agent n'aurait pas assez de temps pour exercer ses fonctions car il ne travaille que dans un régime de 4/5"*.

155. Le défendeur nie que le délégué à la protection des données ne disposerait pas d'assez de temps, compte tenu notamment de l'avis émis dans le dossier qui fait l'objet de la présente procédure. La Chambre Contentieuse constate que le RGPD n'exige pas qu'un délégué à la protection des données soit occupé à temps plein.<sup>38</sup> L'avis du délégué est en outre rédigé de façon détaillée. La Chambre Contentieuse estime que les pièces présentées ne permettent pas de déduire qu'il soit question d'une violation de l'article 38.2 du RGPD.

156. D'après l'article 38.3 du RGPD, le délégué ne peut pas recevoir d'instructions en ce qui concerne l'exercice de ses missions et il fait directement rapport au niveau le plus élevé de la direction du responsable du traitement. En réponse aux questions du Service d'Inspection, le défendeur a communiqué ce qui suit : *"Au sein de Westtoer, un collaborateur a été désigné pour intervenir en tant que personne de contact pour le délégué. Le délégué est associé de façon ad hoc - par téléphone ou par e-mail - via cette personne de contact à la mise en œuvre du RGPD au sein de Westtoer et rend un avis à cette personne de contact conformément à l'article 38, paragraphe 3"*. Le Groupe 29 a déjà souligné l'importance de pouvoir faire rapport au plus haut responsable en ces termes : *"Une telle reddition de compte directe garantit que l'encadrement supérieur (par ex., le conseil d'administration) a connaissance des avis et*

---

<sup>37</sup> Annexes 11 et 12 par e-mail du défendeur au Service d'Inspection du 18 août 2020.

<sup>38</sup> Voir aussi le Groupe 29, Lignes directrices concernant les délégués à la protection des données (DPD), WP 243 rev.01.

*recommandations du [délégué à la protection des données] qui s'inscrivent dans le cadre de la mission de ce dernier consistant à informer et à conseiller le responsable du traitement ou le sous-traitant". D'après la réponse du défendeur, le délégué rend avis à une personne de contact au sein de l'organisation du défendeur. Selon la Chambre Contentieuse, la violation de l'article 38.3 du RGPD est ainsi établie. Aucune violation n'a été constatée à l'article 38.6, vu que le délégué à la protection des données n'exerce pas d'autres tâches et compétences pour le défendeur.*

### **Publication de la décision**

157. Vu l'importance de la transparence concernant le processus décisionnel de la Chambre Contentieuse, conformément à l'article 95, § 1<sup>er</sup>, 8<sup>o</sup> de la LCA, la présente décision est publiée sur le site Internet de l'Autorité de protection des données en mentionnant les données d'identification du défendeur<sup>39</sup>, et ce en raison de la spécificité de la présente décision - ce qui rend inévitable la réidentification, même en cas de suppression des données d'identification - ainsi que de l'intérêt public de cette décision.

### **PAR CES MOTIFS,**

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

- que le système de caméras intelligentes déployé par le défendeur ne comporte aucune violation de l'article 5.1 a), b) et c) et est conforme à l'article 25 du RGPD ;
- d'ordonner au défendeur, conformément à l'article 58.2, d) du RGPD et à l'article 100, § 1<sup>er</sup>, 9<sup>o</sup> de la LCA de mettre les informations qu'il fournit au sujet de ses traitements dans sa déclaration de confidentialité en conformité avec les articles 12 et 13 du RGPD, en particulier en ce qui concerne les informations complémentaires qui sont demandées à la personne concernée dans le cadre d'une demande sur la base des articles 15 à 21 inclus du RGPD (article 12.6 du RGPD), les bases juridiques du traitement (art. 13.1 c) du RGPD) ainsi que les délais de conservation des données à caractère personnel collectées (art. 13.2 a) du RGPD), et ce dans un délai d'un mois à compter de la notification de la présente décision et d'en informer la Chambre Contentieuse dans le même délai ;
- en vertu de l'article 58.2, d) du RGPD et de l'article 100, § 1<sup>er</sup>, 9<sup>o</sup> de la LCA, d'ordonner au défendeur de mettre son registre des activités de traitement en conformité avec les exigences de l'article 30 du RGPD et en particulier de spécifier les pays tiers vers lesquels

---

<sup>39</sup> En omettant toutefois le nom du délégué à la protection des données du défendeur.

des transferts de données sont effectués dans un délai d'un mois après la notification de la présente décision et d'en informer la Chambre Contentieuse dans ce même délai ;  
et

- en vertu de l'article 100, § 1<sup>er</sup>, 5<sup>o</sup> de la LCA, de formuler une réprimande vis-à-vis du défendeur suite à la violation des articles 6.1 a), 7.1, 7.3 (consentement cookies) et 38.3 du RGPD (rapport direct au niveau le plus élevé de la direction du responsable du traitement).

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

(sé.) Hielke Hijmans

Président de la Chambre Contentieuse