



Chambre Contentieuse

**Décision quant au fond 82/2020
du 23 décembre 2020**

Numéro de dossier : DOS-2019-05498

Objet : Plainte concernant la nécessité de créer un compte Microsoft pour télécharger un document du SPF Finances

La Chambre Contentieuse de l'Autorité de protection des données, constituée de Monsieur Hielke Hijmans, président, et de Messieurs Jelle Stassijns et Christophe Boeraeve, 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 :

- M. Willem Debeuckelaere, domicilié à [...] ci-après "le plaignant", et
- le SPF Finances, ayant le numéro d'entreprise 0308.357.159, et dont le siège se situe à 1030 Bruxelles (Schaerbeek), Boulevard du Roi Albert II, 33 boîte 10 (North Galaxy), ci-après "le défendeur" ; ayant pour conseils Maître Agnès Maqua, avocate, et Maître Willem-Jan Cosemans, avocat, ayant tous deux leur bureau à 1170 Bruxelles, Chaussée de la Hulpe, 166.

1. Faits et procédure

La plainte

1. Dans sa plainte du 24 octobre 2019, le plaignant exprime son objection à l'égard d'une pratique sur le site Internet du SPF Finances. Cette pratique exige des citoyens (en tant que personnes concernées) de se connecter avec un compte utilisateur Microsoft¹ afin d'accéder à une brochure déterminée, plus précisément "facturer avec exonération de la TVA" (et de pouvoir la télécharger, le cas échéant). Selon le plaignant, cette pratique serait problématique à la lumière du RGPD et plus spécifiquement à la lumière de la recommandation du 6 février 2019 de cette Autorité,² *concernant "L'obligation de créer un compte utilisateur chez Microsoft pour consulter des applications de services publics"*.
2. Avant le dépôt de sa plainte, le plaignant avait lui-même pris contact avec le défendeur au sujet de son objection et joint également à sa plainte des preuves à cet égard.
3. Le 26 septembre 2019, le plaignant a demandé des informations au défendeur au sujet de la pratique faisant l'objet de la plainte. Cette demande d'informations concernait notamment la question de savoir si la recommandation précitée s'appliquait ou non.
4. Le défendeur a communiqué le jour même et a demandé au plaignant de préciser l'hyperlien en question. Le plaignant a fourni l'hyperlien exact au défendeur le 3 octobre 2019. Le plaignant a fourni en outre quelques captures d'écran pour étayer son point de vue.

¹ Lorsque l'on parle de 'Microsoft' dans la présente décision, il s'agit de la personne morale Microsoft Corporation ayant son siège à One Microsoft Way, Redmond (WA 98052-6399) aux États-Unis d'Amérique, avec un établissement en Belgique : Aéroport de Bruxelles National ZN, Bâtiment 1K, 1930 Zaventem et ayant le numéro d'entreprise 0437.910.359 dans la Banque-Carrefour des Entreprises.

² Centre de Connaissances de l'Autorité de protection des données, **Recommandation n° 1/2019**, disponible via : <https://www.autoriteprotectiondonnees.be/publications/recommandation-n-01-2019.pdf>.

5. Le 15 octobre 2019, après consultation du "Service de sécurité de l'information et de protection de la vie privée" du défendeur, le défendeur a fait savoir qu'une nouvelle application ICT était en cours d'élaboration. L'objectif était de parvenir à un système permettant de donner accès à la partie publique de FisconetPlus via MyMinfin. L'identification et l'authentification se feraient alors via le service d'authentification fédéral (Federal Authentication Service, ci-après "FAS"), ce qui permettrait de ne plus devoir créer un compte Microsoft. Ce système devait être opérationnel début 2020.

Entre-temps, d'après le défendeur, une solution transitoire avait été introduite depuis le 31 janvier 2019, donnant à l'utilisateur la possibilité d'accéder à cette documentation via un compte anonyme, créé par l'intermédiaire d'un fournisseur de services tiers, à savoir Microsoft.

6. Le 29 octobre 2019, la plainte est déclarée recevable par le Service de Première Ligne et la Chambre Contentieuse en est saisie.

L'enquête du Service d'Inspection

7. Le 29 novembre 2019, la Chambre Contentieuse a demandé une enquête au Service d'Inspection. Dans sa demande en vertu de l'article 94, 1^o de la LCA, la Chambre Contentieuse affirme ce qui suit : "*La Chambre Contentieuse a [...] constaté qu'il y avait une imprécision quant à la position du SPF Finances selon laquelle il est possible, à titre de solution provisoire, d'accéder à la documentation avec un compte anonyme créé par Microsoft sans collecte de données à caractère personnel, plus particulièrement dans quelle mesure il est ou non possible que ce compte soit créé par Microsoft sans collecter des données à caractère personnel, plus particulièrement dans quelle mesure il est ou non possible que ce compte soit véritablement anonyme.*" [NdT : Tous les passages cités dans la présente décision ont été traduits librement par le Secrétariat Général de l'Autorité de protection des données, en l'absence de traduction officielle]."

8. Une fois que le Service d'Inspection a été saisi du dossier en vertu de l'article 63, 2^o de la LCA, il a adressé un courrier directement au Président du Comité de direction du défendeur le 5 décembre 2019 afin d'obtenir quelques renseignements complémentaires. Il s'agissait des questions suivantes (capture d'écran de la lettre du Service d'Inspection) :

Ik nam akte van de stelling in uw mail van 15 oktober ll. dat er een overgangsooplossing zou zijn ingevoerd sinds 31 januari 2019 via een "anonieme account aangemaakt door microsoft zonder verzameling van persoonlijke gegevens".

Mag ik u verzoeken om mij per kerende de hierna vermelde informatie/documenten bezorgen⁴:

1. Graag een gedetailleerde beschrijving van alle maatregelen die de FOD Financien tot op heden nam teneinde al dan niet rekening te houden met de aanbeveling nr 91/2019 van 6 februari 2019. Ik wil in het bijzonder nagaan of de communicatie aangaande de accounts werd aangepast.
2. Graag een concrete beschrijving van de "anonieme account aangemaakt door microsoft zonder verzameling van persoonlijke gegevens". Via welke weblink kan de burger deze raadplegen.
3. Welke waarborgen verschaft microsoft u in dat verband. Ik wens stukken te ontvangen die de afspraken met microsoft in dat verband bewijzen (kopie van eventuele correspondentie, contracten, . .)
4. Op welke grond stelt u dat de voormelde account geen persoonsgegevens verwerkt ? Werd dienaangaande een technische verificatie gedaan door een andere partij dan microsoft en kan u mij hiervan desgevallend de nodige bewijsstukken bezorgen ?
5. Graag kopie van alle aanbevelingen die de functionaris van de FOD Financien richtte aan de hoogste leidinggevende van de organisatie sinds 6 februari 2019. Dit teneinde de werking van de functionaris te onderzoeken in het licht van artikel 39 AVG..

9. Le 10 janvier 2020, le Service d'Inspection de l'APD reçoit une réaction écrite du défendeur. Les réponses du défendeur sont formulées comme suit :

(Question 1) "À la réception de la recommandation de l'Autorité de protection des données, le SPF Finances a, dans une première phase :

1. *donné accès à un moteur de recherche basique via le portail MyMinfin, sans identification de l'utilisateur (entrée en vigueur au premier trimestre 2019),*
2. *fourni un accès anonyme via un compte anonyme (entrée en vigueur au deuxième trimestre 2019). Dans une deuxième phase, le projet est lancé pour le développement d'une version qui place le contenu public de FisconetPlus sur MyMinfin. Cette version définitive, qui ne nécessite pas de compte anonyme mais qui permet une authentification au moyen d'une identification FAS, remplacera toutes les autres solutions actuelles pour le public externe de FisconetPlus, c'est-à-dire les versions FisconetPlus avec compte Microsoft, le moteur de recherche simple via MyMinfin et la version avec compte Microsoft anonyme."*

(Question 2) "Plusieurs cas sont possibles :

1. *L'utilisateur a déjà ouvert l'accès au portail (via un compte enregistré ou la solution anonyme). Dans ce cas, le fait de cliquer sur un lien donnera directement accès au document.*
2. *L'utilisateur a ouvert en ayant encore l'accès au portail, il reçoit un message dans lequel on demande de s'identifier. Soit l'utilisateur a un compte et s'identifie. Il a accès aux documents. Soit l'utilisateur n'a pas de compte ou ne souhaite pas créer de compte, l'utilisateur peut copier l'URL et recourir à la possibilité d'un accès anonyme via MyMinFin, comme mentionné à la réponse 2.*
3. *L'utilisateur peut également noter le titre du document qu'il souhaite consulter et utiliser le moteur de recherche disponible via MyMinfin."*

(Questions 3 et 4) "Début janvier 2019, un accès anonyme à FisconetPlus a été prévu. Son objectif est que plus aucune donnée à caractère personnel ne soit demandée à la personne qui souhaite accéder à l'application. Il ne peut dès lors pas se poser de problème pour le traitement de données qui n'existe pas. L'on se réfère à la réponse 2 pour ce qui est du contenu du compte Microsoft anonyme."

(Question 5) "La décision de construire un nouvel environnement technique afin d'accéder à Fisconet, sans devoir utiliser un compte Microsoft, a été prise en interne par le SPF Finances le 14 janvier 2019 (après des réunions préparatoires en décembre 2018). Cette décision a été prise, en présence du DPO, conjointement par le Président du Comité de direction, le Directeur du service d'appui ICT et le Directeur chargé de diriger l'Administration générale Expertise et Support stratégiques. La décision a été communiquée à Microsoft le même jour. Étant donné que les solutions techniques temporaires et définitives ont été prises en conformité avec la recommandation n° 91/2019 du 6 février 2019, il n'était pas nécessaire d'adresser une autre recommandation au Président du Comité de direction. Par contre, à la mi-février 2019 (les 12, 13, 19 et 21 février), des e-mails ont été échangés entre le Président du Comité de direction et le DPO concernant la recommandation précitée (n° 91/2019). La recommandation a été communiquée avec la décision d'adapter l'accès à Fisconet. En outre, les 23 et 24 octobre 2019, le DPO a informé le Président du Comité de direction par e-mail d'une part, des demandes du [plaignant], et d'autre part, de la plainte du [plaignant] auprès de l'Autorité de protection des données."

10. Le 17 janvier 2020, le Service d'Inspection adresse un courrier spécifiquement au délégué à la protection des données (ci-après : DPO) du défendeur pour lui poser quelques questions. Le Service d'Inspection affirme dans ce courrier qu'aucune réponse concrète n'a été donnée aux questions 3, 4 et 5. Le DPO du défendeur est prié de transmettre ces réponses ainsi que les

documents étayant le point de vue du défendeur selon lequel *"les solutions (temporaires) sont conformes à la recommandation 1/2019"*.

11. Le 4 février 2020, le DPO du défendeur répond au Service d'Inspection. Les éléments essentiels de cette réponse peuvent être résumés comme suit :

- En ce qui concerne les questions 3 et 4 : *"le Service d'encadrement ICT a confirmé qu'à aucun moment l'utilisateur ne donne une quelconque information sur lui-même, Microsoft ne dispose donc pas d'information personnelle ou privée. ICT ne m'a pas fourni de copie de documents, mails, ... avec Microsoft"*.³
- En ce qui concerne la question 5, le DPO du défendeur affirme ce qui suit : *"J'ai moi-même fait le projet de réponse à la question 5 et j'estime qu'il y est répondu concrètement. Je ne peux fournir des documents qui n'existent pas."*⁴
- En ce qui concerne la recommandation de l'APD, le défendeur affirme que la décision interne du défendeur (concernant le passage d'outils Microsoft à une solution développée en interne) date du 14 janvier 2019. Cette date est antérieure à la recommandation de l'APD du 6 février 2019.
- Le DPO du défendeur affirme que ces nouvelles solutions sont compatibles avec la recommandation. La technique utilisée précédemment ne l'était toutefois pas. Le DPO affirme ce qui suit : *"Lors de l'analyse du deuxième projet de recommandation soumis par l'APD au SPF Finances le 7 février 2019, j'ai effectivement constaté que la solution technique utilisée auparavant n'était pas compatible avec ce projet mais que les décisions d'adaptation prises par le SPF Finances allaient, elles, dans le sens de la recommandation"*.⁵ Cela s'inscrit plus précisément dans le cadre des § 2, 3 et 4, point 15 de la recommandation.
- Ensuite, le DPO déclare que : *"Ces nouvelles solutions techniques nécessitant des moyens budgétaires (dépassant les 180.000 €) et humains, deux solutions temporaires ont été mises en œuvre le plus rapidement possible à savoir - une consultation simple via MyMinfin, - une consultation via la création d'un compte anonyme chez Microsoft. La version consolidée de consultation via MyMinfin sans authentification a été mise en production fin janvier 2020. La version avec authentification est prévue pour fin mars 2020. Il n'y a pas eu d'évaluation des solutions temporaires proposées. Une évaluation pourra avoir lieu après la mise en œuvre des 2 solutions définitives d'accès offertes."*⁶
- Enfin, une brève explication est donnée au sujet de l'indépendance du DPO et de la manière dont il se positionne au sein du défendeur.

³ Extrait de la réponse rédigée en français.

⁴ Extrait de la réponse rédigée en français.

⁵ Extrait de la réponse rédigée en français.

⁶ Extrait de la réponse rédigée en français.

12. Le Service d'Inspection procède ensuite à quelques constatations techniques. Le rapport d'enquête technique suit le 28 avril 2020, le rapport d'enquête le 11 mai 2020. Le Service d'Inspection a procédé à une série de constatations au cours de la période allant du 7 avril au 20 avril 2020.

Le rapport du Service d'Inspection

13. Le rapport d'enquête du Service d'Inspection est transmis à la Chambre Contentieuse le 11 mai 2020, conformément à l'article 91, § 2 de la LCA.

14. Les *deux premières constatations* (constatations 1 et 2) établies par le Service d'Inspection concernent l'existence de trois possibilités d'accès au service FisconetPlus via deux sites Internet. Il y aurait (eu) trois manières d'accéder à FisconetPlus :

- accès via le site Internet www.myminf.be avec authentification via le FAS ;
- accès via le site Internet www.myminf.be sans authentification (la partie publique de FisconetPlus) ;
- accès via le site Internet général du SPF Finances avec un compte Microsoft personnel ("accès Sharepoint Online").

Le Service d'Inspection relève qu'il s'agit d'un schéma d'accès complexe.

15. Dans les *Constatations 3 et 4*, le Service d'Inspection examine la qualification du défendeur en tant que responsable du traitement, au sens de l'article 4, 7) du RGPD. Le Service d'Inspection en conclut que le défendeur est responsable du traitement pour les traitements qui ont lieu via la plateforme Microsoft intégrée sur son site Internet.

16. *Les constatations 5 à 7 inclus du rapport d'enquête concernent l'utilisation de cookies. Ces constatations sont en lien avec quelques constats du rapport technique.*

Le rapport technique a examiné en premier lieu le site Internet ayant l'URL suivante : <https://eservices.minfin.fgov.be/myminf-web/pages/fisconet>. Au moment des constatations techniques, ce site Internet utilise une bannière de cookies qui affirme que si un utilisateur poursuit la navigation, il accepte l'utilisation de cookies (ce qu'on appelle "further browsing"). À la lumière du RGPD, il doit y avoir une déclaration claire ou un acte positif de l'utilisateur pour avoir un consentement libre, spécifique, clair et univoque.

Non seulement la technique du "further browsing" mais aussi la politique de cookies du défendeur soulève des questions dans le chef du Service d'Inspection. Il fait les constats suivants à cet égard : *"Dans la politique, il n'y a aucune différenciation entre les différents types de cookies ou traceurs. Impossible pour l'utilisateur d'avoir l'information sur les différents cookies, mais aussi sur les cookies pour lesquels il a droit d'exprimer son consentement. (Cookies non strictement nécessaires)."*⁷ Une comparaison entre les cookies énumérés dans la politique de cookies et les cookies chargés à l'ouverture du site Internet révèle que les premiers ne sont pas complets (exhaustifs) et ne sont pas non plus entièrement corrects.

Par ailleurs, le rapport technique se penche aussi sur le site Internet ayant comme URL : <https://finances.belgium.be/fr/E-services/fisconetplus>. Ici aussi, le Service d'Inspection constate une situation en matière de cookies qui est selon lui problématique à la lumière du RGPD. Il y a en effet un décalage entre les cookies énumérés dans la politique de cookies et ceux qui sont effectivement chargés à l'ouverture du site Internet.

Le rapport d'enquête du Service d'Inspection formule trois problèmes quant à l'utilisation de cookies par le défendeur.

- Premièrement, le défendeur considère que le 'further browsing' est un consentement valable pour l'utilisation de cookies sur les deux sites Internet, même si ces cookies ne sont pas nécessaires au bon fonctionnement du ou des site(s) Internet. Ce 'further browsing' est toutefois considéré par le défendeur comme un consentement valable dans sa 'bannière de cookies'. Poursuivre son utilisation du site n'est toutefois pas identique à un consentement.
- Deuxièmement, le Service d'Inspection constate une conséquence à cet égard : étant donné qu'aucun consentement valable n'est demandé pour le placement de cookies, il ne peut pas non plus être prouvé, de sorte que le principe de responsabilité n'est pas respecté. C'est problématique à la lumière de l'article 5, deuxième alinéa et de l'article 7, premier alinéa du RGPD.
- Troisièmement, les visiteurs de sites Internet ne sont pas informés de la manière dont un consentement donné peut être retiré et aucun mécanisme de retrait de consentement n'est prévu. Cette constatation s'applique de nouveau aux deux sites Internet. On se réfère à cet égard à l'article 7, troisième alinéa du RGPD ainsi qu'à la décision 12/2019 de la Chambre Contentieuse.⁸

17. Les constatations 8 à 11 inclus du rapport d'enquête comportent quelques constats concernant l'anonymat des comptes utilisateur en question et le principe de loyauté. Un visiteur du site Internet "<https://finances.belgium.be/fr/E-services/fisconetplus>" aura ainsi le choix de créer un

⁷ Extrait du rapport technique rédigé en français.

⁸ Décision de la Chambre Contentieuse 12/2019 du 17 décembre 2019.

compte personnel et les informations qui y sont fournies donnent l'impression qu'il peut créer un "compte anonyme".

18. L'enquête technique a par contre démontré qu'il n'existerait pas de 'compte anonyme'. Si l'utilisateur choisit l'option "une recherche rapide (anonyme)", il revient sur le site Internet www.myminf.be. La seule alternative qui fonctionne sur le deuxième site Internet est, selon le Service d'Inspection, l'utilisation d'un compte chez Microsoft. En outre, la politique de cookies sur le site Internet général du SPF Finances renvoie à l'utilisation desdits cookies statistiques de Google analytics (types "_ga" "_gat" et "_gid") qui sont utilisés pour distinguer les utilisateurs entre eux de sorte que selon le rapport d'enquête technique, il ne peut pas être question de comptes anonymes.⁹
 19. Ensuite, le Service d'Inspection constate (constatation 8) que les informations que le défendeur a fournies le 15 juin 2018 à l'APD au sujet de l'impossibilité de se connecter anonymement à la plateforme Sharepoint de Microsoft ne correspondent pas aux informations précitées que le défendeur fournit sur son site Internet www.financien.belgium.be aux utilisateurs, ni aux constatations du rapport technique. De plus, les visiteurs du site Internet du défendeur ne sont pas correctement informés du fait que Microsoft ne permet pas des accès anonymes sur la plateforme Sharepoint Online, comme communiqué précédemment à l'APD (constatation 9 du rapport du Service d'Inspection).
 20. Par ailleurs, le compte Microsoft n'est pas véritablement anonyme en raison de cookies placés par le défendeur (constatation 10). De cette manière, les termes "une recherche rapide (anonyme)" ne correspondent pas vraiment à quelque chose d' 'anonyme', donnant à l'utilisateur une présentation erronée de la situation (constatation 11).
 21. Le Service d'Inspection estime que la combinaison de ces éléments mène à la conclusion que le défendeur fournit en permanence des informations inexactes aux personnes concernées. Le défendeur violerait ainsi le principe de loyauté de l'article 5, premier alinéa, point a) du RGPD.
 22. Dans la *constatation 13*, le Service d'Inspection affirme qu'il y a une violation du principe de limitation des finalités (article 5, premier alinéa, point b) et article 32 du RGPD). Le Service d'Inspection constate en effet que le défendeur fournit à Microsoft plus de données à caractère personnel que nécessaire, dont l'adresse e-mail personnelle (que Microsoft utilise pour envoyer le mail d'invitation), et n'en informe pas la personne concernée.
-

23. Dans la *constatation 14*, le Service d'Inspection estime que le défendeur viole l'obligation d'information au sens de l'article 13, premier alinéa, point f) du RGPD. D'après les constatations du rapport d'enquête technique du Service d'Inspection, il y a un flux de et vers Microsoft, ce dont l'utilisateur n'est pas informé de manière transparente. Il s'agit notamment des données d'authentification et de l'adresse e-mail de la personne concernée ainsi que de ses informations de profil (le nom et le prénom de la personne concernée). Ces flux de données sont cachés à l'utilisateur.
24. *La constatation 15 porte sur l'obligation de transparence qui incombe au défendeur ainsi que sur l'obligation d'informer l'utilisateur de manière compréhensible, en des termes clairs et simples (respectivement l'article 5, premier alinéa, point a) et l'article 12, premier alinéa du RGPD). Le Service d'Inspection constate en premier lieu qu'il y a un manuel d'utilisateur imprécis concernant les trois possibilités d'accès. Sur la base des informations disponibles, il ne serait pas clair non plus pour l'utilisateur de déterminer la différence entre ces trois possibilités d'accès. Indépendamment du manuel, les choix qui s'offrent à l'utilisateur ne sont pas expliqués simplement et clairement. Le Service d'Inspection souligne dans le rapport d'enquête que les informations sont trop fragmentées et éparpillées, de sorte que la procédure d'accès peut être considérée comme un 'dédale d'informations'. Enfin, le Service d'Inspection pointe également le constat selon lequel les données à caractère personnel de personnes concernées sont transférées à Microsoft lors du choix sur le deuxième site Internet. Il existe donc bel et bien une différence entre les deux sites Internet, selon le Service d'Inspection.*
25. Le Service d'Inspection affirme dans le rapport d'enquête que le défendeur ne respecte pas le principe de responsabilité de l'article 5, deuxième alinéa du RGPD. Le rapport du Service d'Inspection affirme ce qui suit à ce sujet : "*Le Service d'Inspection a dès lors demandé au SPF Finances, par courrier du 5 décembre 2019, quelles garanties Microsoft lui avait fournies à cet égard, et si une preuve pouvait en être fournie (pièce 7). Il n'a au départ pas reçu de réponse à cette question. Ce n'est qu'après un rappel qu'il a reçu la réponse du délégué indiquant qu'il n'avait pas reçu de pièces du service ICT, ce qui ne constitue pas une réponse directe à la question (page 1 de la pièce 12). Le Service d'Inspection considère cette réponse comme un indice de mépris de l'obligation de coopération (refus de répondre, article 31 du RGPD), et une preuve de violation du principe de responsabilité (article 5.2 du RGPD).*"
26. *La constatation 16 concerne les constatations du Service d'Inspection quant au respect par le défendeur du principe de minimisation des données, conformément à l'article 5, premier alinéa, point c) du RGPD. Le Service d'Inspection constate que l'APD a souligné dans sa recommandation 01/2019 qu'une obligation d'identification ne peut être imposée que s'il est question de la preuve d'une nécessité et d'un fondement clair en vertu de l'article 6 du RGPD (points 10 et 11 de la*

recommandation précitée). Ensuite, le Service d'Inspection conclut que le défendeur ne respecte pas cette recommandation pour les motifs suivants :

1. Des imprécisions entourent le scénario final pour l'accès à FisconetPlus. Il est dès lors difficile d'en évaluer la proportionnalité.
2. Le remplacement des trois différentes possibilités d'accès par une seule, à savoir le système d'authentification FAS, n'est pas conforme au point 10 de la recommandation 01/2019.
3. Le remplacement des trois différentes possibilités d'accès par deux options ne peut pas conduire à une présentation erronée de la situation. Le défendeur doit ainsi veiller au fait qu'il ne peut pas présenter simplement ces deux options à titre d'alternatives (une anonyme, une non anonyme), alors que *de facto* l'utilisateur (via l'utilisation de cookies) est toujours identifié (quelle que soit l'option qu'il choisit).
4. L'accès aux services Cloud Microsoft doit se faire via un compte Microsoft et n'est, en soi, pas nécessaire.
5. Il n'y a pas de nécessité de continuer à fonctionner simultanément avec deux services d'authentification différents (via le FAS et via Microsoft).
6. Le fait de continuer à fonctionner avec le service de Microsoft pendant encore plus d'un an après la publication de la recommandation de l'APD ne peut pas non plus s'expliquer par une "situation transitoire" temporaire vu qu'elle dure depuis plus d'un an.

Le Service d'Inspection estime qu'il y a violation du principe de minimisation des données ainsi que du principe de proportionnalité.

27. *Constatation 17 – À la lumière de l'article 25 du RGPD, le Service d'Inspection affirme que le défendeur n'offre pas le choix le plus respectueux de la vie privée de manière claire et à titre de choix par défaut (accès direct à la base de données de connaissances FisconetPlus sans authentification). Dès lors, le Service d'Inspection estime qu'il y a violation de l'article 25 en ce qui concerne la protection des données dès la conception et la protection des données par défaut.*
28. *Les Constatations 18 et 19 du rapport d'enquête concernent la non-exécution par le défendeur d'une analyse d'impact relative à la protection des données conformément à l'article 35 du RGPD (mieux connue en anglais sous la dénomination 'data protection impact assessment', et dès lors abrégée ci-après DPIA ou AIPD). Le DPO du défendeur affirme à ce sujet à l'égard du Service d'Inspection : "Après examen, il nous semble qu'aucune analyse d'impact relative à la protection des données (DPIA) ne doit être réalisée, étant donné qu'il n'est pas probable que le traitement en question implique un grand risque pour les droits et libertés des personnes concernées, vu sa*

nature, sa portée et son contexte." Le DPO estime en d'autres termes que les conditions pertinentes qui nécessitent la réalisation d'une telle DPIA ne sont pas remplies.

Se basant sur sa propre analyse ainsi que sur la recommandation 01/2019 de l'APD, le Service d'Inspection affirme qu'une DPIA aurait dû avoir lieu pour les traitements en question (la création d'un compte Microsoft pour accéder à FisconetPlus).

29. *Les Constatations 20 et 21 concernent la position du DPO du défendeur (article 38, premier alinéa du RGPD et article 39 du RGPD). Le Service d'Inspection constate que le défendeur a violé l'article 38, premier alinéa du RGPD, étant donné que son DPO n'a pas été impliqué en temps opportun dans l'adaptation du service FisconetPlus (Constatation 20). Le Service d'Inspection renvoie aussi à sa correspondance entre lui-même et le défendeur, d'où il ressort qu'il n'y a pas de point de vue clairement distinct (avis, point de vue, ...) entre celui du DPO et la réponse de la présidence du défendeur (Constatation 21).*
30. À la lumière de l'article 31 du RGPD et de l'article 66, § 2 de la LCA, soit des dispositions juridiques qui détaillent l'obligation de coopération du responsable du traitement, le Service d'Inspection affirme dans le rapport d'enquête que le défendeur doit coopérer avec l'autorité de contrôle lors de l'accomplissement de ses missions. Cela implique que les réponses données à l'APD doivent être dûment analysées et ne peuvent pas être manifestement fausses et potentiellement trompeuses. Dans un premier temps, le Service d'Inspection n'a pas reçu de réponse à certaines de ses questions, dans un deuxième temps, il a reçu une réponse manifestement erronée, ce qu'il considère dès lors comme problématique à la lumière de l'obligation de coopération.
31. Le 18 mai, le Service d'Inspection adresse une ordonnance de **suspension temporaire** au défendeur, conformément à l'article 70 de la LCA. Le défendeur est ainsi sommé de suspendre FisconetPlus, plus spécifiquement l'accès à ce service via la plateforme Gcloudbelgium.sharepoint.com de Microsoft. La mesure vaut pour une durée de 3 mois à partir de la date de réception de la lettre recommandée. Aucun recours n'a été introduit par le défendeur contre cette mesure provisoire, conformément à l'article 71, premier alinéa de la LCA.
32. Le 2 juin 2020, le Président du Comité de direction du défendeur fait savoir au Service d'Inspection que l'accès à FisconetPlus via la plateforme Gcloudbelgium.sharepoint.com a été désactivé depuis le 29 mai 2020 et que l'accès n'est désormais plus possible que via le portail MyMinfin.

La procédure devant la Chambre Contentieuse

33. Le 11 mai 2020, le Service d'Inspection transmet le dossier à la Chambre Contentieuse.
34. Le 4 juin 2020, les parties sont informées de la décision de la Chambre Contentieuse de traiter le dossier sur le fond, conformément aux articles 98 e.s. de la LCA. La lettre adressée aux parties fixe les délais dans lesquels les conclusions ainsi que les moyens de défense doivent être déposés. Les conseils du défendeur demandent une prolongation des délais de conclusions le 3 juillet 2020, après quoi la Chambre Contentieuse procède à un nouvel établissement des délais de conclusions à une date ultérieure, étant donné qu'elle estime que la demande du défendeur est raisonnable.
35. Le vendredi 14 août 2020, le défendeur transmet ses conclusions en réponse. En raison d'un problème technique, l'e-mail contenant les conclusions et ses annexes n'est pas parvenu en temps utile à la Chambre Contentieuse. Le plaignant a quant à lui bien reçu les conclusions le 14 août 2020.
36. Étant donné que le plaignant a pu prendre connaissance des conclusions et des pièces du défendeur en temps opportun, et a même pu introduire des conclusions en réplique sur cette base, il n'était pas nécessaire de redéfinir les délais pour les conclusions. Après avoir constaté le problème technique, la Chambre Contentieuse a réclamé les conclusions en réponse du défendeur et les a ensuite reçues et ajoutées au dossier le 7 octobre 2020.

Les conclusions du plaignant

37. Le 4 novembre 2020, le plaignant dépose ses conclusions. Le plaignant est l'ancien président de la Commission de la protection de la vie privée (ci-après : CPVP) et de l'APD.
38. Le plaignant affirme qu'il vise à préserver l'accès à des informations du secteur public de l'intervention d'un fournisseur de services tiers. Le plaignant déclare que c'est entre-temps le cas, de sorte que cet objectif est atteint. Néanmoins, la situation n'était pas la même au moment de l'introduction de la plainte. À ce sujet, le plaignant se réfère à quelques éléments et preuves du dossier et plus particulièrement aussi à sa propre plainte et aux captures d'écran qu'il a jointes.
39. La plainte se fonde intrinsèquement sur une violation de la recommandation 01/2019 de l'APD, selon le plaignant.
40. Le plaignant souligne que la plainte ne repose sur aucune connaissance quelconque que le plaignant aurait dans le chef de sa fonction d'ancien président de la CPVP, prédécesseur en droit

de l'APD.¹⁰ Le plaignant se réserve le droit de se défendre contre cette accusation de violation de l'obligation de confidentialité de l'article 48, § 1^{er} de la LCA.

41. Le plaignant estime que le défendeur ne respecte en outre pas l'article 25, deuxième alinéa du RGPD, du fait qu'il ne propose pas clairement le mécanisme alternatif du compte anonyme.

Les conclusions du défendeur

42. Le 25 septembre 2020, les conclusions en réplique du défendeur sont transmises. Le défendeur demande à la Chambre Contentieuse de classer la plainte sans suite, et au moins de la déclarer non fondée. Le défendeur demande à la Chambre Contentieuse de déclarer non recevables, ou du moins non fondées, les constatations complémentaires du Service d'Inspection (qui dépassent le cadre de la plainte) – ainsi que toute conséquence juridique à cet égard.

43. Les conclusions du défendeur commencent par une présentation des parties. Le défendeur souligne ici que le plaignant était président de la CPVP et directeur du Centre de Connaissances de l'Autorité de protection des données, au cours de la période précédant l'introduction de la plainte.

44. Le défendeur explique également le service FisconetPlus. Il s'agit d'un portail intégré au G-Cloud fédéral, développé via SharePoint Online, un outil numérique géré par Microsoft. Ce dernier exige la création d'un compte utilisateur pour accéder à sa plateforme. Microsoft a interdit un accès anonyme. Dans la perspective de l'utilisation de cette plateforme, le défendeur a été contacté par l'APD, suite à quoi une solution d'abord temporaire et ensuite définitive a été adoptée.

45. La solution temporaire consiste en trois possibilités d'accès :

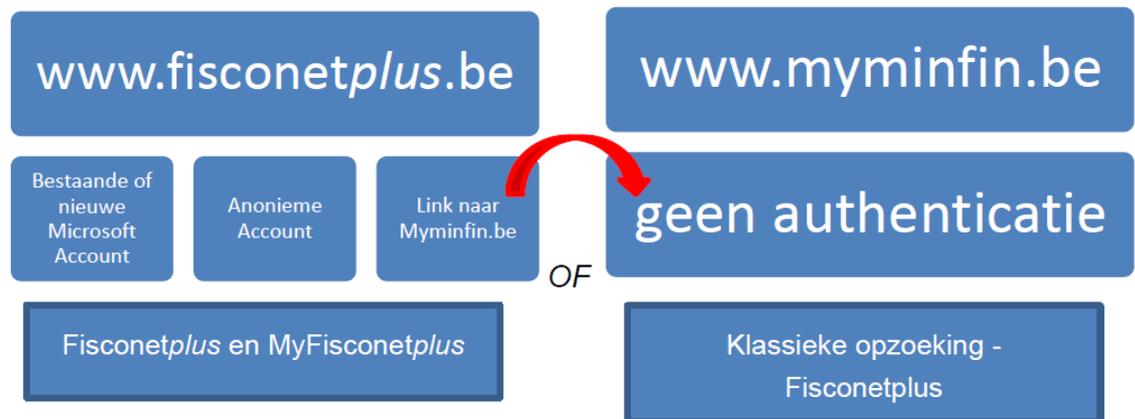
A. Un accès via le moteur de recherche basique de FisconetPlus via Myminf.be, sans aucune authentification : l'utilisateur clique sur un lien le conduisant à une page où il peut effectuer des recherches simples.

B. (À partir du 31 janvier 2019) accès à FisconetPlus via un compte anonyme : le défendeur affirme que cette option a été mise en évidence sur le site Internet, de sorte que l'utilisateur soit mené à l'option la plus respectueuse de la vie privée. L'utilisateur clique sur "créer un utilisateur anonyme" et reçoit ensuite un nom d'utilisateur et un mot de passe aléatoire qu'il doit conserver lui-même. L'utilisateur ne doit pas introduire lui-même des données à caractère personnel.

C. Accès via un compte Microsoft.

¹⁰ Compar. article 3, alinéa 2 de la LCA.

Le défendeur illustre les options d'accès au moyen de la présentation schématique suivante¹¹ :



46. Par ailleurs, le défendeur souligne qu'il n'y a quoi qu'il en soit aucun problème quant à la solution définitive envisagée, étant donné que cette solution implique l'intégration complète des informations sur une propre plateforme, sans intervention d'un quelconque fournisseur de services tiers. Le défendeur affirme à cet égard : *"Le président du défendeur a également informé clairement l'Autorité dès les premiers contacts que les développements précités devaient être réalisés au fur et à mesure, en fonction des moyens disponibles et des différentes directions concernées. Étant donné l'absence actuelle d'un Gouvernement de plein exercice, impliquant des difficultés supplémentaires et des délais plus longs pour obtenir des budgets, ainsi que la crise du Covid-19 à laquelle nous sommes confrontés, ces développements prennent plus de temps que prévu initialement. Au niveau technique aussi, il n'est pas évident de mettre en œuvre à très court terme la solution définitive précitée qui est la plus souhaitable. Ils envisagent à cet égard un délai de 9 à 12 mois"*.

47. Après un aperçu de la procédure préalable, le défendeur en vient à ses arguments concrets. Nous reprenons ci-dessous les 22 moyens que le défendeur invoque :

48. "MOYEN 1 : "OBSCURI LIBELLI" ET NON-RECEVABILITE DES ACTIONS EN JUSTICE"

Le défendeur affirme que la Chambre Contentieuse a mis plus de six mois après le dépôt de la plainte pour demander pour la première fois au défendeur de faire connaître ses moyens de défense, bien qu'entre-temps, il y a eu notamment une mesure provisoire prise par le Service d'Inspection à l'égard du défendeur, conformément à l'article 70 de la LCA. Le défendeur estime que *"l'on ne peut pas du tout savoir clairement quels actes [lui] sont **précisément** reprochés."*

¹¹ Extrait des conclusions en réplique du défendeur

49. *"MOYEN 2 : L'AUTORITÉ A VIOLÉ L'ARTICLE 54.2 DU RGPD ET L'ARTICLE 48, § 1 DE LA LOI APD DU FAIT QUE SES MEMBRES N'ONT PAS RESPECTÉ L'OBLIGATION DE PRÉSERVER LE CARACTÈRE CONFIDENTIEL DES FAITS, ACTES OU RENSEIGNEMENTS DONT ILS ONT EU CONNAISSANCE EN RAISON DE LEURS FONCTIONS"*

Le défendeur affirme qu'il "ressort clairement et manifestement du dossier que le plaignant a utilisé des faits et des éléments du dossier dont il avait pris connaissance précédemment en sa qualité de président de l'Autorité et de directeur du Centre de Connaissances." Selon le défendeur, le plaignant a des connaissances préalables particulières au sujet d'éléments du dossier et les utilise pour porter plainte ultérieurement en tant que citoyen. Le défendeur se réfère notamment à cet égard à l'article 48, § 1^{er} de la LCA et à l'article 54, deuxième alinéa du RGPD et estime que l'on peut constater une violation de ces dispositions juridiques dans le chef du plaignant.

50. *"MOYEN 3 : UNE RECOMMANDATION N'A PAS DE FORCE LÉGALE – MÉPRIS DE COMPÉTENCES ET DE RÉPARTITION DES TÂCHES AU SEIN DE L'AUTORITÉ"*

Le défendeur précise son moyen invoqué comme suit : "en rédigeant une recommandation [1/2019] en sa qualité de directeur du Centre de Connaissances d'une part, et en portant plainte pour non-respect de cette même recommandation d'autre part, le plaignant a violé différents principes juridiques et les tâches confiées spécifiquement au Centre de Connaissances."

Le défendeur estime par ailleurs que le but n'est pas de régler une situation spécifique via une recommandation, nonobstant les compétences d'avis et de recommandation de l'APD. En outre, une recommandation n'a pas de force juridique contraignante.

51. *"MOYEN 4 : PROCÈS INÉQUITABLE, VIOLATION DES DROITS DE LA DÉFENSE ET IMPARTIALITÉ"*

Le défendeur affirme que ses droits de la défense sont systématiquement ignorés. Le défendeur souligne que le plaignant est l'ancien président de l'APD, ce qui compromet la licéité de la procédure et l'impartialité des membres de la Chambre Contentieuse.

Le défendeur attire également l'attention sur le nouveau site Internet de l'Autorité de protection des données, qui a été lancé pendant la procédure, et qui a rendu inaccessibles toute une série de publications pertinentes pour la défense, ce qui a entraîné "une nouvelle atteinte à l'égalité des armes."

52. *"MOYEN 5 : L'AUTORITÉ A VIOLÉ LES PRINCIPES DE BONNE ADMINISTRATION AINSI QUE LE PRINCIPE DE SÉCURITÉ JURIDIQUE"*

Depuis mars 2018, l'APD était au courant de l'existence du nouveau portail FisconetPlus, selon le défendeur. Finalement, des réunions ont également eu lieu en décembre 2018 entre le défendeur et l'APD. À ce moment, aucune objection n'a été formulée au sujet des solutions temporaires et définitives.

Malgré cela, le 20 mai 2020, le Service d'Inspection impose soudainement au défendeur une ordonnance de suspension temporaire concernant l'accès à FisconetPlus. Les conseils du défendeur affirment qu'un laps de temps trop court a été octroyé pour développer un nouveau système. Aucune concertation préalable n'a eu lieu avec le défendeur et aucun délai ne lui a été octroyé.

53. *"MOYEN 6 : CHARGE DE LA PREUVE"*

Le Service d'Inspection n'a pas établi de procès-verbal au sens de l'article 67 de la LCA. Le défendeur affirme que les constatations du Service d'Inspection n'ont pas (ou ne peuvent pas avoir) de force probante particulière et souligne que par chaque moyen, il peut apporter la preuve contraire des constatations contestées.

54. *"MOYEN 7 : L'AUTORITÉ A VIOLÉ L'ARTICLE 63 DE LA LCA DU FAIT QUE LE SERVICE D'INSPECTION A MENÉ UNE ENQUÊTE SUR DES ASPECTS DONT IL N'A PAS ÉTÉ SAISI"*

Le défendeur renvoie ici à la demande de la Chambre Contentieuse à l'égard du Service d'Inspection, conformément à l'article 94, 1^o de la LCA, qui était bien plus limitée que l'enquête finale et aux constatations finales faites par le Service d'Inspection, telles que reprises dans le rapport abordé précédemment.

55. *"MOYEN 8 : L'AUTORITÉ A VIOLÉ L'ARTICLE 96, § 1^{ER} DE LA LCA DU FAIT QUE LA DEMANDE DE LA CHAMBRE CONTENTIEUSE DE FAIRE RÉALISER UNE ENQUÊTE PAR LE SERVICE D'INSPECTION N'A PAS ÉTÉ ADRESSÉE À L'INSPECTEUR GÉNÉRAL DU SERVICE D'INSPECTION DANS LES TRENTE JOURS APRÈS QUE LA CHAMBRE CONTENTIEUSE A ÉTÉ SAISIE DE LA PLAINTÉ PAR LE SERVICE DE PREMIÈRE LIGNE"*

Le défendeur affirme que cette demande a été adressée après 31 jours, ce qui dépasse le délai prévu dans la loi. Dès lors, le rapport d'inspection ainsi que les pièces en annexe du rapport d'inspection doivent être exclus des débats, selon le défendeur.

56. *"MOYEN 9 : LA PLAINTÉ EST NON RECEVABLE ET À TOUT LE MOINS NON FONDÉE"*

La plainte concerne le fait que la brochure ne peut être consultée qu'en créant un compte Microsoft. Le défendeur rétorque que le Service d'Inspection a affirmé dans son rapport que l'objection du plaignant *"n'a pas été prouvée"*. Le fait que des captures d'écran fournies par le plaignant indiquent la possibilité de créer un compte Microsoft n'implique en effet pas qu'il y a une obligation de créer un compte Microsoft.

Par ailleurs, le défendeur affirme que le principe selon lequel l'accès à des informations du secteur public devrait être exempté de l'intervention de fournisseurs de services tiers ne figure pas dans le RGPD.

57. *"MOYEN 10 : L'ACCÈS AU SERVICE FISCONETPLUS NE SUIT PAS UN SCHEMA D'ACCÈS COMPLEXE"*

Le rapport d'inspection conclut que si l'on présente schématiquement tous les choix d'accès sur FisconetPlus et MyMinfin, on obtient un schéma d'accès complexe.¹² Dès lors, l'accès au service FisconetPlus suivrait un schéma d'accès complexe qui n'est pas transparent pour l'utilisateur. Le défendeur le conteste et affirme qu'il a respecté correctement l'obligation de transparence.

58. *"MOYEN 11 : LE DÉFENDEUR EST RESPONSABLE DU TRAITEMENT, SOIT SEUL, SOIT CONJOINTEMENT POUR CERTAINS TRAITEMENTS DE DONNÉES À CARACTÈRE PERSONNEL – MICROSOFT EST RESPONSABLE DU TRAITEMENT POUR CERTAINS TRAITEMENTS DE DONNÉES À CARACTÈRE PERSONNEL"*

En ce qui concerne l'application Sharepoint Online Cloud de Microsoft, les conventions contractuelles entre le défendeur et Microsoft qualifient le défendeur de responsable du traitement et qualifient Microsoft de sous-traitant, d'après le défendeur.

Néanmoins, le défendeur estime que certaines précisions doivent être apportées, spécifiquement en ce qui concerne l'authentification via le compte Microsoft. Premièrement, le défendeur souligne le fait qu'au moment du choix d'intégrer FisconetPlus à l'application Sharepoint Online Cloud de Microsoft, il n'était pas requis de se connecter avec un compte Microsoft pour accéder à l'application Sharepoint Online Cloud. Pour des raisons de sécurité, Microsoft a ensuite fait ce choix et l'a implémenté structurellement au niveau mondial. Il ne s'agit pas du choix du défendeur. Deuxièmement, Microsoft a confirmé au défendeur que pour toute authentification se faisant via le compte Microsoft, Microsoft agissait en tant que responsable du traitement.

¹² Le défendeur renvoie à cet égard au rapport technique d'enquête du Service d'Inspection, p.5.

Le défendeur estime qu'il s'agit d'une responsabilité distincte à l'égard du traitement, Microsoft étant responsable pour certains aspects et le défendeur pour d'autres aspects. Le défendeur ne serait ainsi pas responsable de la méthode d'authentification prescrite par Microsoft.

59. *"MOYEN 12 : LES INFORMATIONS DANS LA POLITIQUE DE COOKIES SONT COMPLÈTES, TRANSPARENTES ET CORRECTES"*

Le Service d'Inspection affirme que la politique de cookies n'est pas complète et n'est pas (entièrement) correcte. En réalité, des cookies ne figurant pas dans la politique de cookies seraient placés. Le défendeur insiste sur le fait qu'il ne s'agit que d'un seul cookie non mentionné ; il s'agit d'un cookie de sécurité (*session cookie*).

60. *"MOYEN 13 : POUR LES COOKIES PLACÉS PAR LE DÉFENDEUR, AUCUN CONSENTEMENT N'EST NÉCESSAIRE – AU BESOIN, LE CONSENTEMENT A ÉTÉ OBTENU VALABLEMENT"*

Le défendeur affirme que tous les cookies que le défendeur place via son site Internet (dont aussi les cookies qui ont été constatés par le Service d'Inspection) sont des cookies essentiels ou fonctionnels.

Dès lors, il n'est pas exigé de demander le consentement des personnes concernées en vertu de l'article 129 de la loi relative aux communications électroniques (en exécution de l'article 5.3 de la directive vie privée et communications électroniques).¹³ Si un consentement était quand même exigé, il est obtenu valablement par le défendeur. La bannière de cookies demande en effet le consentement de la personne concernée en cliquant sur "Oui, je suis d'accord" et précise que la personne concernée donne son consentement en poursuivant activement la navigation sur le site Internet. Il s'agit ainsi bel et bien d'un consentement explicite et actif. Les conseils du défendeur affirment dès lors que les constatations 5 et 6 du rapport d'inspection ne sont pas correctes.

61. *"MOYEN 14 : LE SERVICE D'INSPECTION NE FOURNIT PAS DE PREUVE QUE LE COMPTE ANONYME VIA FISCONETPLUS N'ÉTAIT PAS ANONYME"*

Le défendeur objecte que le Service d'Inspection indique à plusieurs endroits de son rapport que *"le compte 'anonyme' n'était pas véritablement anonyme, sans démontrer vraiment cette affirmation."* Le défendeur se réfère ici à l'analyse du Service d'Inspection dans laquelle ce dernier constate que le placement de cookies par Microsoft après connexion via un compte utilisateur

¹³ Loi du 13 juin 2005 *relative aux communications électroniques*, M.B. 20 juin 2005 (**LCE**) ; Directive (UE) 2002/58/CE du 12 juillet 2002 *concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques*, J.O. UE L/37 (**directive vie privée et communications électroniques**).

implique que l'utilisation du compte n'est pas vraiment anonyme. Il n'y a toutefois pas eu d'analyse par le Service d'Inspection du compte "anonyme", selon le défendeur.

Le défendeur affirme en outre dans ce cadre que certaines constatations du Service d'Inspection ne sont pas exactes. Le rapport du Service d'Inspection ne contient pas d'analyse technique du compte anonyme et en outre, le Service d'Inspection n'indique pas quels cookies comportent des données à caractère personnel ou sont associés à un identifiant, comme une adresse IP.

62. *"MOYEN 15 : LA POLITIQUE DE COOKIES PRÉVOIT BIEN UNE EXPLICATION QUANT À LA MANIÈRE DONT UN CONSENTEMENT DONNÉ PEUT ÊTRE RETIRÉ AINSI QU'UN MÉCANISME DE RETRAIT DE CONSENTEMENT"*

Selon le Service d'Inspection, les deux sites Internet ne donneraient pas d'explication au sujet du (retrait du) consentement pour l'utilisation de cookies. Le défendeur affirme qu'aucun consentement ne doit être obtenu de la part de la personne concernée pour le placement de cookies essentiels et fonctionnels. Le défendeur prévoit toutefois une explication sur la manière de supprimer les cookies.

63. *"MOYEN 16 : PAS DE VIOLATION DES PRINCIPES DU RGPD"*

Les conseils du défendeur affirment que les déclarations du défendeur sont mal présentées dans le rapport. Dès lors, selon le défendeur, le principe de loyauté repris à l'article 5, premier alinéa, point a) du RGPD n'a pas été violé et différentes constatations du Service d'Inspection ne sont pas correctes.

Les constatations du Service d'Inspection concernant le respect du principe de finalité (article 5, premier alinéa, point b) du RGPD) et la sécurité suffisante des données à caractère personnel (article 32 du RGPD) ne sont pas correctes et relèvent de suppositions erronées.

Le défendeur se réfère également au Manuel d'utilisateur de son site Internet pour argumenter que – contrairement aux constatations faites par le Service d'Inspection – l'obligation d'information de l'article 13, premier alinéa du RGPD a bien été respectée. En l'espèce, le défendeur affirme que les destinataires de données à caractère personnel étaient clairement indiqués et qu'aucune donnée à caractère personnel n'a été transmise en dehors de l'Union.

64. *"MOYEN 17 : PAS DE VIOLATION DE L'OBLIGATION DE COOPÉRATION"*

Le défendeur affirme qu'il a dûment respecté ses obligations au sens de l'article 31 du RGPD et de l'article 66 de la LCA.

65. *"MOYEN 18 : PAS DE VIOLATION DE L'OBLIGATION DE MINIMISATION DES DONNÉES"*

Le défendeur souligne que la connexion au portail FisconetPlus présentait pour les utilisateurs l'avantage de bénéficier de services personnalisés (comme la conservation et la catégorisation de documents).

66. *"MOYEN 19 : PAS DE VIOLATION DES PRINCIPES DE PROTECTION DES DONNÉES DÈS LA CONCEPTION ET DE PROTECTION DES DONNÉES PAR DÉFAUT"*

Le défendeur répète qu'au moment de son choix de la plateforme Sharepoint de Microsoft pour le développement, la connexion au moyen d'un compte utilisateur n'était pas requise, et qu'il s'agissait d'un choix de Microsoft, et donc que l'on ne peut pas lui reprocher une violation de l'article 25 du RGPD.

67. *"MOYEN 20 : IL N'ÉTAIT PAS NÉCESSAIRE DE RÉALISER UNE ANALYSE D'IMPACT RELATIVE À LA PROTECTION DES DONNÉES"*

D'après le défendeur, il *"n'est pas question d'un 'risque potentiellement élevé'"* au sens de l'article 35 du RGPD et le traitement ne relève pas non plus d'une des situations de l'article 35 du RGPD. Par ailleurs, le défendeur souligne que le traitement ne figure pas non plus sur la liste des traitements nécessitant une AIPD, établie par l'Autorité de protection des données.

68. *"MOYEN 21 : DÉLÉGUÉ"*

Le défendeur affirme que la position du DPO est suffisamment indépendante au sein du modèle organisationnel du défendeur, conformément aux articles 37 et 38 du RGPD, et qu'il a toujours réalisé correctement ses tâches au sens de l'article 39 du RGPD.

Le défendeur souligne également que le Service d'Inspection aurait lui-même créé une confusion en écrivant d'abord au Président du Comité de direction. Le DPO n'a pas été contacté directement par écrit en première instance et n'a donc pas répondu directement aux questions du Service d'Inspection.

69. "MOYEN 22 : À TITRE SUBSIDIAIRE : APPLICATION CLÉMENTE"

À titre subsidiaire, le défendeur demande à la Chambre Contentieuse de procéder à une application clémente de ses compétences.

Le défendeur demande en ordre principal :

1. de classer la plainte sans suite en application de l'article 100, § 1^{er}, 1^o de la LCA, ou du moins de déclarer la plainte non fondée ;
2. de déclarer les constatations complémentaires – et toute conséquence juridique de celles-ci – comme non recevables, ou du moins non fondées, et dès lors d'ordonner le non-lieu en application de l'article 100, § 1^{er}, 2^o de la LCA.

Le défendeur demande à titre subsidiaire :

1. d'ordonner la suspension du prononcé, en application de l'article 100, § 1^{er}, 3^o de la LCA.

Le défendeur demande à titre plus subsidiaire :

2. de formuler des avertissements et des réprimandes, en vertu de l'article 100, § 1^{er}, 5^o de la LCA.

L'audition

70. Par arrêté ministériel du 28 octobre 2020 *portant des mesures d'urgence pour limiter la propagation du coronavirus COVID-19 (M.B. du 28/10/2020)*, les autorités fédérales ont pris plusieurs mesures contraignantes compliquant l'organisation d'une audition avec toutes les parties dans la composition habituelle. La Chambre Contentieuse a dès lors offert aux parties la possibilité d'organiser l'audition par voie électronique. Les deux parties ont confirmé leur présence à l'audition au préalable, conformément à l'article 51 du Règlement d'ordre intérieur de l'Autorité de protection des données.

71. L'audition a eu lieu le 16 novembre 2020. Les deux parties étaient présentes.

72. Un procès-verbal de l'audition a été dressé, dont le seul but est de donner des compléments d'information et des précisions concernant les conclusions déposées antérieurement. Comme toujours, les parties ont également eu la possibilité de formuler des remarques factuelles sur le procès-verbal, sans impliquer une réouverture des débats. Le défendeur a transmis de telles remarques qui ont été ajoutées au dossier en annexe au procès-verbal.

3. Motivation

a. La compétence du Service d'Inspection et de la Chambre Contentieuse et l'ampleur du dossier

i. La requête du défendeur d'exclure des pièces des débats

73. Le 29 octobre 2019, le Service de Première Ligne a déclaré la plainte recevable et l'a transmise à la Chambre Contentieuse, en vertu de l'article 62, § 1^{er} de la LCA. Le 24 novembre 2019, la Chambre Contentieuse a conclu qu'une enquête du Service d'Inspection était nécessaire, en application de l'article 94, 1^o et de l'article 63, 2^o de la LCA. Le 29 novembre 2019, la demande de procéder à une enquête a été transmise au Service d'Inspection, conformément à l'article 96, § 1^{er} de la LCA.

74. Dans le moyen 8 de ses conclusions en réplique, le défendeur affirme que le rapport du Service d'Inspection, ainsi que les pièces en annexe au rapport, doivent être exclus des débats, en raison de la transmission tardive par la Chambre Contentieuse de la demande à l'égard du Service d'Inspection de procéder à une enquête. La plainte a en effet fait l'objet d'une saisine par le Service de Première Ligne le 29 octobre 2019, soit 31 jours avant la demande au sens de l'article 96, § 1^{er} de la LCA.

La Chambre Contentieuse considère le délai visé à l'article 96, § 1^{er} de la LCA, dont le dépassement n'est frappé d'aucune sanction dans la norme juridique proprement dite, comme un délai d'ordre. Le dépassement du délai ne constitue pas en soi la nullité des actions suivantes d'une autorité administrative¹⁴. La Chambre Contentieuse ne voit dès lors pas la nécessité d'exclure des débats le rapport du Service d'Inspection, ainsi que les pièces apportées par le Service d'Inspection, et de ne pas les prendre en considération dans la délibération visant à prendre la présente décision, d'autant plus que le dépassement du délai (en l'espèce tout juste 1 jour) ne porte pas atteinte à un intérêt du défendeur protégé juridiquement.

75. Ne fût-ce que pour la protection juridique des personnes concernées (citoyens), et plus particulièrement compte tenu du droit des personnes concernées de porter plainte conformément à l'article 77, premier alinéa du RGPD, et des missions et pouvoirs de traiter cette plainte, attribuées à l'autorité de contrôle conformément aux articles 57 et 58 du RGPD, on ne peut en

¹⁴ Compar. Cass. Arrêt du 27 juin 2019 (disponible via juportal.be): "Ce délai, qui n'est assorti d'aucune sanction, est un délai d'ordre dont le dépassement n'a pas pour conséquence de rendre l'amende administrative illégale."

autre accepter qu'une disposition de procédure nationale prévoyant un délai d'ordre prive ainsi l'autorité de contrôle de ces missions et pouvoirs.¹⁵

- ii. *Les moyens du défendeur en matière d' "obscuri libelli", de "non-recevabilité des actions en justice" et des compétences d'enquête du Service d'Inspection dans un dossier contenant une plainte*

76. Suite à son enquête, le Service d'Inspection fait en effet plusieurs constatations dans son rapport qui concernent le même défendeur (en tant que responsable du traitement) que celui mentionné dans la plainte, bien que ces constatations ne se rapportent pas – ou du moins pas toujours – directement à l'objet de la plainte.

77. Dans le premier moyen de ses conclusions en réplique, le défendeur argumente que la plainte concerne un seul aspect, mais que le Service d'Inspection examine de nombreux aspects, de sorte que pour le défendeur *"on ne peut pas du tout savoir clairement quels actes sont **précisément** reprochés au défendeur"*.

Dans le septième moyen de ses conclusions en réplique, le défendeur affirme que *"l'autorité a violé l'article 63 de la LCA du fait que le Service d'Inspection a mené une enquête sur des aspects dont il n'a pas été saisi"*.

78. Une fois que le Service d'Inspection est saisi du dossier par la Chambre Contentieuse conformément à l'article 63, 2^o de la LCA, il dispose en effet de la compétence d'analyser plus avant les traitements liés à l'objet de la plainte. On peut souligner à cet égard que le simple fait que la plainte concerne l'accès à une brochure spécifique ne peut pas limiter les compétences d'enquête du Service d'Inspection (articles 64 à 90 inclus de la LCA) à une simple constatation de l'exactitude de la plainte. Les compétences d'enquête doivent en effet servir à examiner le respect des dispositions en matière de protection des données à caractère personnel. Pour cette raison, l'enquête doit au moins aussi pouvoir porter sur des éléments qui sont accessoires à l'objet de la plainte.

79. La Chambre Contentieuse souligne par ailleurs que lorsque le Service d'Inspection constate au cours d'une enquête portant sur une plainte qu'il y a des indices sérieux de l'existence d'une pratique pouvant donner lieu à une violation des principes fondamentaux de la protection des

¹⁵ En ce qui concerne la protection juridique des citoyens sur la base du droit de l'Union et des principes d' 'action directe' et de 'primauté', voir notamment l'Arrêt CJUE 5 février 1963, *NV Algemene Transport- en Expeditie Onderneming van Gend & Loos c. Nederlandse Administratie der Belastingen*, C-26-62, ECLI:EU:C:1963:1; CJUE, Arrêt du 15 juillet 1964, *Flaminio Costa c. E.N.E.L.*, C-6-64, ECLI:EU:C:1964:66 ; voir également la doctrine à ce sujet : C. BARNARD, *The Substantive Law of the EU: The Four Freedoms*, Oxford (5^e éd.), 2016, 17.

données à caractère personnel, le Service d'Inspection peut examiner de nouveaux éléments de sa propre initiative, conformément à l'article 63, 6° de la LCA. La Chambre Contentieuse précise toutefois que dans l'affaire en cause, toutes les constatations du Service d'Inspection se rapportent directement ou indirectement à l'objet de la plainte et toutes les constatations font partie d'un seul dossier, dont a été saisi le Service d'Inspection sur la base de l'article 63, 2° de la LCA.

80. On ne peut pas non plus affirmer en l'espèce que l'ampleur du dossier n'était pas claire pour le défendeur, dès lors que la décision de la Chambre Contentieuse du 4 juin 2020 invitant les deux parties à transmettre leurs conclusions conformément aux articles 98 et 99 de la LCA, renvoie clairement à la plainte ainsi qu'aux constatations du Service d'Inspection.¹⁶

81. La demande de la Chambre Contentieuse à l'égard du Service d'Inspection ne limite donc aucunement l'ampleur de l'enquête ni les possibilités d'enquête de ce service. Cela ressort clairement du texte de loi. Pour cette raison, l'argument tiré du moyen 1 des conclusions en réplique du défendeur ne peut être accepté. En outre, la Chambre Contentieuse précise par souci d'exhaustivité que la LCA ne prévoit aucunement la possibilité de déclarer une plainte "irrecevable" pour ainsi dire *a posteriori* – après avoir été déclarée recevable par le Service de Première Ligne.¹⁷

b. L'indépendance et l'intégrité des collaborateurs et des membres de l'Autorité de protection des données dans son ensemble, et de la Chambre Contentieuse en particulier (article 54, deuxième alinéa du RGPD et article 48, § 1^{er} de la LCA)

82. Dans le deuxième moyen de ses conclusions en réplique, le défendeur affirme que l'APD a elle-même violé l'article 54, deuxième alinéa du RGPD ainsi que l'article 48, § 1^{er} de la LCA *"du fait que ses membres n'ont pas respecté l'obligation de préserver le caractère confidentiel des faits, actes ou renseignements dont ils ont eu connaissance en raison de leurs fonctions"*.

83. Pour étayer cet argument, le défendeur renvoie à la communication – qu'il joint lui-même – entre lui-même et le plaignant en sa qualité de président et directeur de l'APD (et précédemment président de la CPVP), et en particulier à une lettre datant du 15 juin 2018. En outre, on souligne que la recommandation 1/2019 sur laquelle le plaignant fonde sa plainte a été signée par le

¹⁶ La lettre adressée au défendeur mentionne entre autres littéralement : *"Sur la base de la plainte et des constatations faites par le Service d'Inspection, la Chambre Contentieuse décide de procéder à un examen quant au fond."*

¹⁷ La Chambre Contentieuse a par ailleurs bien la compétence de décider que l'on ne peut constater aucune infraction et, en vertu de l'article 100, § 1, 2° de la LCA, d'ordonner le non-lieu ou de classer la plainte sans suite, conformément à l'article 95, § 1, 1° ou à l'article 100, § 1, 1° de la LCA (selon le stade de la procédure auquel le dossier se trouve).

plaignant en sa qualité de directeur du Centre de Connaissances.

84. La Chambre Contentieuse souhaite avant tout préciser que l'APD, Chambre Contentieuse incluse, effectue ses tâches de manière transparente et intègre, utilisant comme seuil minimal l'obligation légale d'intégrité, reprise à l'article 54, deuxième alinéa du RGPD et à l'article 48, § 1^{er} de la LCA, dispositions légales auxquelles le défendeur se réfère. Le défendeur affirme à tort qu'il est question d'un procès inéquitable, d'une violation des droits de la défense et d'impartialité.¹⁸
85. La Chambre Contentieuse souligne notamment la politique constante qu'elle applique en matière de publication de ses décisions – avec ou sans suppression des données d'identification et sous réserve de la compétence décisionnelle des membres siégeant de publier ou non la décision dans un dossier individuel –, dans le cadre de laquelle elle rend publiques, dans la mesure du possible, ses activités et décisions après clôture de dossiers de manière transparente pour les citoyens.¹⁹ La présente décision sera ainsi également publiée (voir ci-après.).
86. Lors de la prise de la décision, toutes les pièces du dossier sont prises en considération et lors de l'évaluation du dossier, la Chambre Contentieuse ne se limite donc aucunement aux éléments à charge.²⁰ Lors de l'évaluation intrinsèque du dossier et des délibérations qui ont précédé la présente décision, il a toujours été tenu compte des arguments et des conclusions du défendeur, ainsi que des réponses et des pièces fournies par le défendeur au Service d'Inspection et qui font partie intégrante du dossier.
87. Le plaignant n'est actuellement pas membre ni membre du personnel de l'APD et n'est pas impliqué dans les activités intrinsèques de l'Autorité, et ne l'était pas non plus au moment de la plainte. Il a introduit une plainte au départ de son adresse e-mail privée. Il faut faire la distinction entre la qualité professionnelle (antérieure ou non) du plaignant et sa qualité de citoyen de l'Union européenne et du Royaume de Belgique. Aucune législation européenne ou nationale ne prive le plaignant du droit de porter plainte auprès d'une autorité de contrôle, en l'espèce l'APD, conformément à l'article 77 du RGPD, du fait qu'il est ou a été impliqué lui-même dans le fonctionnement de cette autorité. Cela s'applique *a fortiori* pour les personnes qui ont travaillé à l'APD par le passé (récent), mais qui n'en font plus partie.

¹⁸ Plus particulièrement dans le moyen 4 des conclusions en réplique du défendeur.

¹⁹ La Chambre Contentieuse décide au cas par cas quant à la publication des décisions, conformément à l'article 95, § 1, 8^o et à l'article 100, § 1, 16^o de la LCA, selon le stade de la procédure dans lequel le dossier se trouve.

²⁰ Moyen 4 des conclusions en réplique défendeur : "*le dossier a été mené exclusivement à charge du [défendeur], sans que les différents rapports ne montrent que [le défendeur] a toujours coopéré avec l'Autorité dans ce dossier.*"

88. Par ailleurs, il n'est nullement question du fait que le plaignant soit *"donc juge et partie' dans un même litige"*, comme le défendeur l'argumente dans ses conclusions en réplique.²¹ Les membres de la Chambre Contentieuse nommés par la Chambre des représentants statuent de manière indépendante et autonome dans chaque dossier pour lequel ils siègent, conformément à l'article 52 du RGPD et aux articles 43 e.s. de la LCA.
89. Les membres soulignent qu'aucune influence externe n'a été exercée sur eux lors du traitement de ce dossier et que les membres n'ont accepté aucune instruction quelconque de qui que ce soit dans le cadre du traitement de ce dossier.²² On peut également souligner qu'au moment où le plaignant exerçait des activités (en tant que directeur) pour la CPVP ou l'APD, les membres siégeant dans ce dossier n'étaient pas simultanément employés ou membres nommés de l'APD.
90. Le défendeur affirme dans ses conclusions en réplique que : *"Le plaignant fait clairement usage de ses connaissances préalables particulières du dossier (...). La plainte ne mentionne effectivement aucune référence explicite à des éléments confidentiels du dossier, mais il est toutefois clair que les connaissances préalables du plaignant quant au dossier ont joué un rôle décisif pour le plaignant dans le dépôt de sa plainte."*
91. On peut souligner que dans sa plainte ou à d'autres stades du traitement du dossier à l'APD, le plaignant n'a soumis aucune preuve illicite, et qui plus est, il ne s'est appuyé que sur des documents disponibles publiquement. La lettre du 15 juin 2018 à laquelle le défendeur se réfère a été apportée par le défendeur lui-même et n'a pas été soumise par le plaignant afin d'exercer ses droits en tant que citoyen.
92. Bien entendu, il est un fait qu'en tant qu'ancien président et directeur respectivement de la CPVP et de l'APD, le plaignant a une certaine expertise au niveau de la protection des données à caractère personnel et a pu ainsi identifier et soumettre des documents publics pertinents. Le simple fait qu'un citoyen maîtrise bien la législation et la réglementation en la matière en raison de ses activités professionnelles et utilise ces connaissances pour exercer ses droits en tant que citoyen ne signifie toutefois pas *ipso facto* que cette personne abuse de ses droits ou viole des obligations d'intégrité (qui découlent de ses activités professionnelles).
93. La Chambre Contentieuse ne voit dès lors aucun motif pour lequel une infraction à l'article 54, deuxième alinéa ou à l'article 48, § 1^{er} de la LCA aurait été commise par le plaignant ou l'APD

²¹ Moyen 2 des conclusions en réplique défendeur.

²² Compar. article 52, deuxième alinéa du RGPD et article 43, premier alinéa de la LCA.

elle-même ; l'argument du deuxième moyen des conclusions en réplique du défendeur ne peut donc pas être retenu.

c. Le(s) responsable(s) du traitement au sens de l'article 4, point 7) du RGPD

94. La Chambre Contentieuse procède à la désignation du responsable du traitement pour les traitements concernant l'objet de la plainte et les constatations du Service d'Inspection dans son rapport. Conformément à l'article 4, point 7) du RGPD, le responsable du traitement est :

"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; lorsque les finalités et les moyens de ce traitement sont déterminés par le droit de l'Union ou le droit d'un État membre, le responsable du traitement peut être désigné ou les critères spécifiques applicables à sa désignation peuvent être prévus par le droit de l'Union ou par le droit d'un État membre".

95. Dans son rapport, le Service d'Inspection affirme que le défendeur est le responsable du traitement pour l'ensemble de la gestion du 'service FisconetPlus', incluant la connexion au moyen d'un compte utilisateur Microsoft (tant via un compte utilisateur anonyme que via un compte utilisateur 'normal'). Le Service d'Inspection affirme que la responsabilité du défendeur comporte "une combinaison de divers choix concernant l'offre de diverses possibilités d'accès impliquant ou non un traitement de données à caractère personnel, à savoir" (capture d'écran sans reprise des notes de bas de page) :

- Het aanbieden van de databank Fisconetplus in verschillende vormen (zowel als "onbeschermde resource"²⁰ als in de vorm van "beschermde resource"²¹;
- de keuze om voor de authenticatiedienst (onder meer) beroep te blijven doen op Microsoft²² (tegelijk met de keuze voor de federale authenticatiedienst FAS);
- het al dan niet herbergen van de authenticatiedienst op infrastructuur van Microsoft;
- het opstellen van de lay-out van de eerste en tweede website;
- de (al dan niet) communicatie van de verplichte informatie hierop aan de betrokken gebruikers (relevant in het licht van de toepassing van de artikelen 12, 13 en 14 AVG).

Traduction libre :

- La mise à disposition de la banque de données FisconetPlus sous différentes formes (aussi bien en tant que "ressource non protégée"²⁰ qu'en tant que "ressource protégée"²¹ ;
- le choix de continuer à recourir à Microsoft²² pour le service d'authentification (notamment) (parallèlement au choix du service d'authentification fédéral FAS) ;
- l'hébergement ou non du service d'authentification sur l'infrastructure de Microsoft ;
- l'établissement de la mise en pages du premier et du deuxième site Internet ;

la communication (ou l'absence de communication) des informations obligatoires aux utilisateurs concernés (ce qui est pertinent à la lumière de l'application des articles 12, 13 et 14 du RGPD).

96. Dans son onzième moyen, le défendeur affirme toutefois que pour un certain nombre de traitements de données à caractère personnel, cités dans le dossier, il peut ne pas être considéré comme responsable du traitement au sens de l'article 4, point 7 du RGPD : *"Le [défendeur] ne conteste pas qu'il est responsable du choix d'intégrer FisconetPlus dans l'application de cloud Sharepoint Online de Microsoft [...] Le [défendeur] n'a aucunement opéré un quelconque choix pour :*

- *continuer à faire appel à Microsoft pour le service d'authentification (notamment) ;*
- *héberger ou non le service d'authentification sur l'infrastructure de Microsoft.*

Ces choix ont été opérés uniquement par Microsoft et le [défendeur] n'avait pas d'autre choix que de poursuivre à ce moment (provisoirement) avec Microsoft."

97. Le défendeur estime que *"Microsoft est responsable du traitement en ce qui concerne toute authentification qui se fait via le compte Microsoft et donc aussi pour toute authentification via le compte Microsoft dans le cadre de FisconetPlus."* Le défendeur se réfère à cet égard à la position de Microsoft en tant que "sous-traitant" au sens de l'article 28 du RGPD, Microsoft devenant responsable du traitement conformément à l'article 28, alinéa 10 du RGPD pour le traitement qui nécessite l'authentification via un compte Microsoft.

98. La Cour de justice a confirmé que pour l'identification du ou des responsables du traitement, il fallait une évaluation factuelle de la ou des personnes physiques ou de la ou des personnes morales qui détermine(nt) "les finalités" et "les moyens" du traitement, la notion étant définie de manière large en vue de protéger les personnes concernées.²³ La cour a également estimé qu'une personne physique qui influe, à des fins qui lui sont propres, sur le traitement de données à caractère personnel et participe de ce fait à la détermination des finalités et des moyens de ce traitement, peut être considérée comme étant responsable du traitement.²⁴

99. La Cour de justice a également confirmé qu'il est possible que, dans le cadre d'un traitement avec des responsables conjoints du traitement, toutes les opérations réalisées avec les données à caractère personnel par les responsables du traitement respectifs ne concernent pas la

²³ Arrêt CJUE du 13 mai 2014, *Google Spain en Google*, C-131/12, ECLI:EU:C:2014:317, par. 34 ; Arrêt CJUE du 5 juin 2018, *Wirtschaftsakademie Schleswig-Holstein*, C-210/16, ECLI:EU:C:2018:388, par. 28.

²⁴ Arrêt CJUE du 10 juillet 2018, *Jehovan todistajat*, C-25/17, ECLI:EU:C:2018:551, par. 68.

responsabilité de chaque responsable du traitement²⁵.

C'est notamment le cas lorsqu'il s'agit d'un responsable du traitement spécifique qui détermine les finalités et les moyens d'une opération spécifique. Cela signifie que cette opération est suffisamment distincte du traitement pour lequel un autre responsable du traitement détermine (conjointement) les finalités et les moyens pour les traitements de données à caractère personnel.

100. Dans le cas présent, la procédure de connexion via Microsoft (tant via un compte 'anonyme' que via un compte utilisateur 'ordinaire') est nécessaire pour l'utilisation de FisconetPlus et de ses possibilités de personnalisation (comme la conservation de documents par les utilisateurs). Lorsqu'au cours des étapes successives – facilitées via un site Internet du défendeur –, des données à caractère personnel sont traitées, ces traitements sont fortement liés aux finalités du site Internet dans son intégralité, déterminées par le défendeur, et au service FisconetPlus qui y est proposé, en particulier.

101. Par ailleurs, c'est le défendeur lui-même qui a conclu les conventions contractuelles pour l'hébergement du service FisconetPlus au moyen du service Sharepoint Online de Microsoft, ce dernier nécessitant l'utilisation d'un compte utilisateur ('anonyme' ou non) pour l'utilisation de ses services. C'est donc le défendeur qui opte pour les services et les produits (numériques) de Microsoft et détermine ainsi les moyens du traitement.

102. Peu importe si à cet égard, il n'était pas nécessaire, au moment de conclure les engagements entre le défendeur et Microsoft, d'utiliser un compte utilisateur ('anonyme' ou non) pour pouvoir utiliser la plateforme Sharepoint Online. Il s'agit d'une question contractuelle entre le défendeur et Microsoft, qui ne porte pas préjudice aux obligations légales de responsables du traitement à l'égard du traitement de données à caractère personnel. L'authentification via le compte utilisateur ('anonyme' ou non) est en effet nécessaire pour utiliser le site Internet du défendeur, le traitement étant indissociablement lié au site Internet et à son propriétaire.

103. Pour le traitement de données à caractère personnel lors de l'utilisation du service FisconetPlus sur Sharepoint Online, incluant l'authentification via un compte utilisateur de Microsoft, le défendeur est donc bien intégralement responsable du traitement au sens de l'article 4, point 7) du RGPD.

104. Cela implique que le défendeur doit respecter ses responsabilités au sens de l'article 5, deuxième alinéa et de l'article 24 du RGPD quant au respect des dispositions du RGPD. Cela vaut aussi

²⁵ Cf. CJUE, arrêt du 29 juillet 2019, *Fashion ID GmbH & Co KG c. Verbraucherzentrale NRW eV*, C-40/17, ECLI:EU:C:2019:629, par. 76.

lorsque Microsoft est également responsable du traitement pour l'authentification et que Microsoft et le défendeur sont responsables conjoints du traitement, conformément à l'article 26 du RGPD.²⁶

d. Le respect des principes relatifs au traitement de données à caractère personnel (article 5 du RGPD) et la protection des données dès la conception et la protection des données par défaut (article 25 du RGPD)

i. L'exigence du respect des principes relatifs au traitement de données à caractère personnel à la lumière de l'article 25 du RGPD

105. La Chambre Contentieuse a repris tous les éléments du dossier dans sa délibération, et conclut que le cœur de la problématique qui a donné lieu à la plainte peut être ramené au respect du principe de loyauté et de transparence du traitement au sens de l'article 5, premier alinéa, point a) du RGPD, d'une part, et au respect du principe de minimisation des données – repris à l'article 5, premier alinéa, point c) du RGPD, d'autre part.

106. Le Service d'Inspection constate à juste titre un certain nombre de problèmes, qui conduisent par exemple à la constatation *"que le [défendeur] permet, lors du transfert de données à caractère personnel à Microsoft, de communiquer plus d'éléments que nécessaire et ne respecte ainsi pas le principe de finalité"*, ainsi qu'à la constatation relative à la sécurité des données à caractère personnel lorsqu'elles sont traitées par Microsoft.²⁷ La Chambre Contentieuse considère que ces problèmes découlent toutefois des problèmes initiaux concernant les dispositions énoncées aux points précédents (et, comme on le motive ci-après, des violations de ces dispositions), tant lors de la détermination des moyens du traitement que lors du traitement proprement dit.

107. Au sens strict du RGPD, il doit y avoir un traitement de données à caractère personnel avant de pouvoir constater une violation de l'article 5 du RGPD. En théorie, il est en effet possible qu'aucune personne concernée ne s'authentifie via un compte utilisateur en introduisant des données à caractère personnel afin d'accéder à FisconetPlus, impliquant l'absence de traitement de données à caractère personnel et impliquant donc aussi que l'on ne puisse pas constater de violation des dispositions relatives à la protection des données à caractère personnel.²⁸

²⁶ Compar. article 26, paragraphe 3 du RGPD : *"Indépendamment des termes de l'accord visé au paragraphe 1, la personne concernée peut exercer les droits que lui confère le présent règlement à l'égard de et contre chacun des responsables du traitement"*.

²⁷ Constatation 13 du rapport du Service d'Inspection.

²⁸ Compar. *mutatis mutandis* la motivation lors de l'annulation d'une décision de la Chambre Contentieuse par la Cour des marchés, où la Chambre Contentieuse avait constaté, dans cette décision, une violation de l'article 5, premier alinéa, point c) du RGPD : arrêt de la Cour d'appel (Chambre 19A) di 19 février 2019, *X c. APD*, n° de rôle 2018/AR/1600, 27 : *"Aucune eID*

108. En l'occurrence, il apparaît, sur la simple base des pièces que le plaignant a soumises, que ce dernier ne se soit pas connecté au moyen d'un compte utilisateur. Les captures d'écran ne montrent en effet que l'écran de connexion et non l'utilisation de FisconetPlus après que le plaignant se soit déjà authentifié.
109. En ce sens, on ne peut accepter, à la lumière des pouvoirs des autorités de contrôle²⁹ ainsi qu'à la lumière de l'importance de la protection des données à caractère personnel³⁰, que la protection juridique de citoyens via l'Autorité de protection des données ne soit possible que lorsqu'un traitement effectif donne lieu à une infraction, et non lorsqu'une personne concernée refuse un traitement déterminé en tant que pratique du fait qu'elle considère qu'il n'est pas conforme avec la garantie de ses propres droits.
110. Le législateur européen a dès lors aussi prévu un article 25 dans le RGPD, qui oblige le responsable du traitement à prendre certaines mesures pour se conformer aux dispositions du RGPD, pour d'éventuels et/ou futurs traitements de données à caractère personnel, et notamment "au moment de la détermination des moyens du traitement".³¹ L'article 25 du RGPD spécifie l'obligation générale d'un responsable du traitement de prendre des mesures techniques et organisationnelles appropriées (le principe de "responsabilité", tel qu'établi à l'article 24 du RGPD).
111. La Chambre Contentieuse considère dès lors le respect des principes relatifs au traitement de données à caractère personnel de l'article 5 du RGPD à la lumière des obligations dans le chef d'un responsable du traitement en vertu de l'article 25 du RGPD, qui dispose ce qui suit :

"1. Compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, 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

n'a en l'occurrence été produite par la plaignante et aucun traitement de ses données n'a donc eu lieu. L'APD ne prouve dès lors aucune violation effective de données à caractère personnel." (soulignement par la Chambre Contentieuse).

²⁹ Spécifiquement l'article 58 du RGPD et les dispositions d'exécution nationales dans la LCA.

³⁰ La protection des données à caractère personnel est reprise à l'article 8 de la Charte des droits fondamentaux de l'Union européenne.

³¹ Pour une explication concernant le lien entre l'article 25 et les principes relatifs au traitement de données à caractère personnel, voir les Lignes directrices 4/2019 du 20 octobre 2020 du Comité européen de la protection des données (EDPB) concernant la protection des données dès la conception et par défaut (v. 2.0.), disponible via : https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf.

minimisation des données, de façon effective et à assortir le traitement des garanties nécessaires afin de répondre aux exigences du présent règlement et de protéger les droits de la personne concernée.

2. 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.

3. Un mécanisme de certification approuvé en vertu de l'article 42 peut servir d'élément attestant du respect des exigences énoncées aux paragraphes 1 et 2 du présent article."
(soulignement par la Chambre Contentieuse)

ii. Le rôle de Microsoft en tant que fournisseur de services tiers et la Recommandation 1/2019

112. Dans ses conclusions en réplique, le défendeur a clairement indiqué que lors de l'utilisation de FisconetPlus, les personnes concernées avaient toujours le choix de s'authentifier au moyen d'un propre compte Microsoft (contenant des données à caractère personnel), ou via un compte Microsoft anonyme, qui ne contient en principe pas de données à caractère personnel, mais le Service d'Inspection a relevé le placement de différents cookies qui porteraient atteinte au caractère anonyme du compte utilisateur.³²

113. Le défendeur indique dans son neuvième moyen que la lecture des dispositions du RGPD n'indique en rien que l'accès à des informations du secteur public doit être exempté de l'intervention d'un fournisseur de services tiers, du moment que le RGPD est respecté. La Chambre Contentieuse considère qu'il ne s'agit pas d'une représentation fidèle de la situation au moment de la plainte, où l'option d'accès à FisconetPlus qui est *de facto* la plus conviviale entraîne une collecte active et un traitement des données à caractère personnel des personnes concernées par le fournisseur de services tiers, afin d'accéder à la plateforme du défendeur. C'est notamment le cas lors de l'utilisation d'un (propre) compte utilisateur Microsoft existant ou nouveau.

114. La base juridique du problème résidant dans le fait que l'intervention notamment de ce fournisseur de services peut être considérée comme problématique dans certains cas, n'est en

³² Pour une explication quant à l'utilisation de cookies par le défendeur, voir ci-après dans la partie 2.6.

effet pas reprise dans des recommandations – comme le défendeur le fait remarquer à juste titre – mais bien dans la législation elle-même. La Chambre Contentieuse souligne toutefois que l'interprétation de la législation requiert un examen des éléments factuels, ainsi qu'une application de la législation à ces éléments, sous la responsabilité du responsable du traitement lors de la détermination des moyens du traitement (article 25, premier alinéa du RGPD).

115. Dans un environnement numérique complexe en évolution permanente au sein duquel des données à caractère personnel sont traitées, le législateur a dès lors prévu un rôle consultatif pour les autorités de contrôle, par exemple pour pouvoir répondre à des questions et besoins sociétaux, ainsi qu'à certaines tendances. La Chambre Contentieuse souligne à cet égard les pouvoirs établis légalement à l'article 58, troisième alinéa du RGPD et le rôle régi concrètement à cet égard pour le Centre de Connaissances de l'APD aux articles 23 e.s. de la LCA.

116. Dans la Recommandation 1/2019 du 6 février 2019, le Centre de Connaissances a en effet émis une recommandation concernant l'obligation de créer un compte utilisateur chez Microsoft pour consulter des applications de services publics, conformément aux dispositions juridiques précitées. Cette recommandation précise ce que la législation requiert dans le chef notamment du défendeur en tant que service public, sans toutefois être contraignante en soi pour le défendeur.

117. La Chambre Contentieuse souligne que dans la présente décision, elle intervient par la sanction à l'égard du défendeur sur la base de la législation, mais aussi que cette législation a été précisée dans une recommandation du Centre de Connaissances et que l'on peut donc difficilement affirmer que l'interprétation concrète de la législation manque de précision. Le défendeur semble d'ailleurs le confirmer lui-même, étant donné qu'il estime que des mesures sont nécessaires après avoir pris connaissance de la Recommandation 1/2019 et qu'il affirme dans ses conclusions en réplique que : *"Après avoir pris connaissance de la recommandation, le SPF Finances a pris des mesures afin de respecter le contenu de cette recommandation. Il a ainsi été décidé dans une première phase de mettre en œuvre une solution intermédiaire qui serait ensuite suivie d'une solution définitive."*³³

118. La Recommandation 1/2019 est destinée à éclairer les responsables du traitement quant à l'interprétation de la norme légale. Dans son troisième moyen de ses conclusions en réplique, le défendeur affirme à juste titre qu'une recommandation n'a pas de valeur légale. Toutefois, une recommandation, en tant que forme de "*soft law*", est un instrument accepté pour clarifier les choses lorsque la norme légale laisse une certaine marge. S'ajoute à cela qu'en l'occurrence, le

³³ Conclusions en réplique du défendeur, point 15.

défendeur ne remet pas en doute l'exactitude de l'explication de la norme légale dans la recommandation.

iii. La violation de l'article 5, premier alinéa, point a) juncto l'article 25 du RGPD

119. La Chambre Contentieuse constate que la collecte et la structuration d'une certaine documentation par les personnes concernées via un site Internet du service public qui a (conjointement) le contrôle de la législation fiscale et de la réglementation fiscale peuvent être sensibles lorsqu'elles sont associées à un citoyen (en tant que personne concernée). On peut ainsi penser à la collecte de certaines informations par la personne concernée dans le cadre de sa défense dans une procédure auprès de ce service public. Dans la présente situation, le défendeur pourrait déduire des informations de certaines recherches effectuées par des citoyens identifiés, qu'il pourrait utiliser à l'encontre du citoyen concerné, dans la détermination de l'impôt à payer.

120. Il va de soi que les données à caractère personnel de la personne concernée qui sont associées à de telles informations doivent être traitées de manière correcte et transparente.

121. Par ailleurs, la Chambre Contentieuse souligne que le défendeur propose bel et bien des informations d'une manière qui ne requiert pas l'utilisation d'un compte utilisateur ('anonyme' ou non) de Microsoft, à savoir via le *"moteur de recherche basique de FisconetPlus via Myminfin.be"*. La Chambre Contentieuse remarque toutefois que ce n'est pas parce qu'il existe une option (offrant par ailleurs moins de fonctionnalités) n'entraînant pas ou moins de traitements de données à caractère personnel, que les possibilités d'accès où des données à caractère personnel sont bel et bien collectées et traitées ultérieurement devraient bénéficier d'une moins bonne protection en vertu du RGPD.

122. La possibilité d'accès aux informations via le moteur de recherche basique sans connexion via un compte utilisateur signifie toutefois qu'il ne peut être question d'une violation de l'article 6, premier alinéa du RGPD, étant donné que l'accès aux informations n'est en soi pas exclu sans l'utilisation d'un compte utilisateur de Microsoft. Le caractère libre du consentement lors de l'utilisation du compte utilisateur Microsoft n'est dès lors pas problématique en l'espèce.

123. Dans son examen réalisé dans le cadre de la rédaction de la Recommandation 1/2019, le Centre de Connaissances a souligné quelques aspects propres à l'utilisation du compte utilisateur Microsoft, impliquant par exemple que des données relatives aux activités de navigation et de

recherche et à d'autres activités en ligne liées au compte Microsoft de l'utilisateur concerné sont utilisées ensuite par Microsoft.³⁴

124. Lorsque l'option d'accès à FisconetPlus qui est la plus conviviale se fait moyennant l'utilisation d'un compte utilisateur ('anonyme' ou non) de Microsoft, on ne peut pas affirmer que les données à caractère personnel des personnes concernées sont traitées de manière transparente et loyale, ni que lors de la détermination des moyens du traitement, des mesures techniques et organisationnelles suffisantes ont été prises pour garantir ces principes, au sens de l'article 5, premier alinéa, point a) *juncto* l'article 25, premier alinéa du RGPD. C'est le cas dès lors qu'une possibilité d'accès requérant un compte utilisateur Microsoft implique que des données à caractère personnel de personnes concernées ne peuvent pas être traitées de manière loyale. En outre, le défendeur n'explique pas de manière suffisamment transparente aux personnes concernées (potentielles) de quelle manière les données à caractère personnel des personnes concernées, et les informations associées qui sont traitées via FisconetPlus sur une plateforme Sharepoint Online, sont utilisées ultérieurement par Microsoft, ne sont pas utilisées ou pourraient être utilisées par affiner ou commercialiser des services et produits (numériques) propres de Microsoft.

La violation de l'article 5, premier alinéa, point c) juncto l'article 25 du RGPD

125. La Chambre Contentieuse a déjà souligné que les circonstances dans lesquelles le défendeur propose les informations sur son site Internet impliquent une certaine sensibilité et requièrent dès lors le soin et les précautions nécessaires lors du traitement de données à caractère personnel associées. La Chambre Contentieuse constate ensuite que la possibilité qu'un compte utilisateur anonyme de Microsoft puisse être utilisé pour se servir de FisconetPlus (où ce compte assorti de données de connexion aléatoires collecte et traite en tout état de cause moins de données à caractère personnel) prouve par définition que l'option d'accès, dans laquelle des données à caractère personnel d'un compte Microsoft existant ou nouveau sont traitées, traite plus de données à caractère personnel que le strict nécessaire au sens de l'article 5, premier alinéa, point c) du RGPD.

126. Pour la raison précitée, le défendeur commet une violation du principe de minimisation des données repris à l'article 5, premier alinéa, point c) *juncto* l'article 25, premier alinéa du RGPD, en offrant aux personnes concernées une possibilité d'accès (qui plus est la plus conviviale) pour laquelle le traitement de données à caractère personnel n'est pas nécessaire au regard des finalités (c'est-à-dire l'accès à FisconetPlus) pour lesquelles elles sont traitées, et avec l'intervention d'un fournisseur de services tiers, à savoir Microsoft, et le traitement par ce service de ces données à caractère personnel.

³⁴ Recommandation 1/2019, point 8.

e. La réalisation d'une Analyse d'impact relative à la protection des données (AIPD, article 35 du RGPD)

127. Le Service d'Inspection souligne dans son rapport la nécessité de réaliser une AIPD. D'après l'argumentation du défendeur, on peut *"conclure qu'il n'était pas nécessaire de réaliser une [AIPD] par le [défendeur] en tant que responsable du traitement au sujet du site Internet de FisconetPlus".*³⁵

128. L'article 35 du RGPD dispose ce qui suit :

1. Lorsqu'un type de traitement, en particulier par le recours à de nouvelles technologies, et compte tenu de la nature, de la portée, du contexte et des finalités du traitement, est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, le responsable du traitement effectue, avant le traitement, une analyse de l'impact des opérations de traitement envisagées sur la protection des données à caractère personnel. Une seule et même analyse peut porter sur un ensemble d'opérations de traitement similaires qui présentent des risques élevés similaires.

2. Lorsqu'il effectue une analyse d'impact relative à la protection des données, le responsable du traitement demande conseil au délégué à la protection des données, si un tel délégué a été désigné.

3. L'analyse d'impact relative à la protection des données visée au paragraphe 1 est, en particulier, requise dans les cas suivants : a) l'évaluation systématique et approfondie d'aspects personnels concernant des personnes physiques, qui est fondée sur un traitement automatisé, y compris le profilage, et sur la base de laquelle sont prises des décisions produisant des effets juridiques à l'égard d'une personne physique ou l'affectant de manière significative de façon similaire ; b) le traitement à grande échelle de catégories particulières de données visées à l'article 9, paragraphe 1, ou de données à caractère personnel relatives à des condamnations pénales et à des infractions visées à l'article 10; ou c) la surveillance systématique à grande échelle d'une zone accessible au public.

4. L'autorité de contrôle établit et publie une liste des types d'opérations de traitement pour lesquelles une analyse d'impact relative à la protection des données est requise conformément au paragraphe 1. L'autorité de contrôle communique ces listes au comité visé à l'article 68.

³⁵ Conclusions en réplique du défendeur, point 191.

5. L'autorité de contrôle peut aussi établir et publier une liste des types d'opérations de traitement pour lesquelles aucune analyse d'impact relative à la protection des données n'est requise. L'autorité de contrôle communique cette liste au comité.

6. Avant d'adopter les listes visées aux paragraphes 4 et 5, l'autorité de contrôle compétente applique le mécanisme de contrôle de la cohérence visé à l'article 63, lorsque ces listes comprennent des activités de traitement liées à l'offre de biens ou de services à des personnes concernées ou au suivi de leur comportement dans plusieurs États membres, ou peuvent affecter sensiblement la libre circulation des données à caractère personnel au sein de l'Union.

7. L'analyse contient au moins :

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 conformément au paragraphe 1 ; et

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 et à apporter la preuve du respect du présent règlement, compte tenu des droits et des intérêts légitimes des personnes concernées et des autres personnes affectées.

8. Le respect, par les responsables du traitement ou sous-traitants concernés, de codes de conduite approuvés visés à l'article 40 est dûment pris en compte lors de l'évaluation de l'impact des opérations de traitement effectuées par lesdits responsables du traitement ou sous-traitants, en particulier aux fins d'une analyse d'impact relative à la protection des données.

9. Le cas échéant, le responsable du traitement demande l'avis des personnes concernées ou de leurs représentants au sujet du traitement prévu, sans préjudice de la protection des intérêts généraux ou commerciaux ou de la sécurité des opérations de traitement. "

10. Lorsque le traitement effectué en application de l'article 6, paragraphe 1, point c) ou e), a une base juridique dans le droit de l'Union ou dans le droit de l'État membre auquel le responsable du traitement est soumis, que ce droit régit l'opération de traitement spécifique ou l'ensemble des opérations de traitement en question et qu'une analyse d'impact

relative à la protection des données a déjà été effectuée dans le cadre d'une analyse d'impact générale réalisée dans le cadre de l'adoption de la base juridique en question, les paragraphes 1 à 7 ne s'appliquent pas, à moins que les États membres n'estiment qu'il est nécessaire d'effectuer une telle analyse avant les activités de traitement.

11. Si nécessaire, le responsable du traitement procède à un examen afin d'évaluer si le traitement est effectué conformément à l'analyse d'impact relative à la protection des données, au moins quand il se produit une modification du risque présenté par les opérations de traitement.

129. La Chambre Contentieuse estime que lors du traitement de données à caractère personnel par le défendeur pour une possibilité d'accès à FisconetPlus avec l'exigence d'utiliser un compte utilisateur Microsoft, il était bel et bien question d'un "risque élevé" pour "les droits et libertés des personnes physiques", comme visé à l'article 35, premier alinéa du RGPD. Plusieurs éléments avancés par le Service d'Inspection mènent à cette conclusion de la Chambre Contentieuse (rapport du Service d'Inspection) :

*"a) Le service FisconetPlus est intégré dans le **G-cloud fédéral**, qui est lui-même développé sur la plateforme Microsoft qui est propriété de Microsoft (page 28 de la pièce 13 et pièce 14). Le propriétaire de *gcloudbelgium.sharepoint.com* est, d'après le rapport technique, Microsoft Corporation (illustrations 18 et 19 de la pièce 13). L'enquête technique de l'APD souligne également le problème que le service FisconetPlus est proposé sur l'infrastructure de Microsoft (remarque sur l'illustration 18 de la pièce 13). Une telle **technologie "hybrid cloud"** proposée par des tierces parties en dehors de l'UE a associé des risques particuliers à des éléments³⁶ que les autorités publiques doivent étudier soigneusement, au moyen de la conclusion de garanties contractuelles supplémentaires et de l'application de normes adaptées qui ont été développées pour la technologie cloud telles que ISO/IEC 17788:2014 et ISO/IEC 17789:2014.*

Pour autant que le Service d'Inspection ait pu le vérifier, le SPF Finances n'a pas appliqué de garanties complémentaires à ce niveau (voir le manque de réponse concrète à ce sujet évoqué au sujet du concept de responsabilité ci-avant).

³⁶ "le lieu des back-ups, la séparation des éléments du traitement qui ne restent pas au sein de l'UE (séparation entre conservation dans l'UE et traitement en dehors de l'UE) ou de parties de la plateforme qui restent bien en Belgique de manière sous-jacente, l'accès de Microsoft aux données, la propriété des clés de cryptage, le manque d'autonomie du SPF Finances lors de

l'utilisation d'une solution standard de Microsoft, l'accès par des organes publics aux USA si Microsoft était soumis

à une citation, le lieu inconnu et le délai de conservation de ces solutions".

[...]

c) De par le transfert d'informations à Microsoft (ou le stockage chez Microsoft), il est question d'opérations qui impliquent en soi une **perte de contrôle pour la personne concernée** sur ses données à caractère personnel et une possibilité réduite d'exercer les droits du RGPD en raison d'un manque de transparence et d'informations inexactes (concernant la possibilité de créer un "compte anonyme") que le SPF Finances fournit à ce sujet concernant les opérations réellement effectuées par Microsoft avec les données à caractère personnel des utilisateurs FiconetPlus avec un compte personnel. Ce qui précède est également illustré par les conditions longuement formulées du compte Microsoft gratuit³⁷ en vertu desquelles l'utilisateur Microsoft accorde une "licence de propriété intellectuelle internationale à titre gratuit pour utiliser son contenu" (et donc aussi ses données à caractère personnel). Il n'y a pas d'éléments indiquant que le SPF Finances a analysé le risque de tierces parties de Microsoft, ou l'a limité par des garanties contractuelles.

d) Le SPF Finances fait **appel en continu à une tierce partie** pour fournir le service (d'authentification), ce qui, combiné à d'autres critères, a un impact accru sur le risque de

violation de données à caractère personnel pour la personne concernée³⁸ (voir page 28 de la pièce 13).

e) Dans le rapport d'enquête technique [...], on démontre que les utilisateurs du service FiconetPlus (via la plateforme Sharepoint) sont **profilés par une entreprise privée qui propose le service d'authentification**. Les informations que la personne concernée a données à Microsoft pour la création d'un compte e-mail Outlook sont utilisées pour créer un

³⁷La page <https://www.microsoft.com/nl-be/servicesagreement/> comporte la disposition suivante "Dans toute la mesure nécessaire pour vous fournir les Services, ou les fournir aux autres (ce qui peut comprendre la modification de la taille, de la forme ou du format de Votre Contenu afin de vous offrir un meilleur stockage ou affichage), vous protéger et protéger les Services, et améliorer les produits et services Microsoft, vous accordez à Microsoft une licence de propriété intellectuelle internationale à titre gratuit pour utiliser

Votre Contenu et, par exemple, le copier, le conserver, le transmettre, modifier son format,

le diffuser via des outils de communications et l'afficher sur les Services. Si vous publiez Votre Contenu dans des zones du Service où il est mis à disposition publiquement en ligne ou sans restrictions, Votre Contenu est susceptible d'apparaître au sein de démonstrations ou de supports visant à promouvoir le Service. Certains des Services sont financés par la publicité. Des contrôles sur la façon

dont Microsoft personnalise la publicité sont disponibles sur la page Sécurité et vie privée du site Internet Microsoft pour la gestion

de compte. Nous n'utilisons pas le contenu de vos e-mails, discussions, appels vidéo, appels audio, documents,

photos ou de tout autre fichier personnel afin de vous adresser des publicités ciblées. Nos politiques relatives à la publicité sont décrites en détail dans la Déclaration de Confidentialité."

³⁸ "Voir la page 7 de l'avis de l'EDPB 05/2018 publié à l'adresse https://edpb.europa.eu/sites/edpb/files/files/file1/2018-09-25-opinion_2018_art_64_de_sas_dpia_list_en.pdf."

*compte FisconetPlus. Si l'utilisateur crée un profil via le deuxième site Internet, le rapport technique d'enquête démontre qu'il est question d'un **profil personnalisé** associé à une adresse e-mail personnalisée de la personne concernée (texte de l'illustration 12 de la pièce 13). Le compte qui est ainsi créé est bien un compte Microsoft. Des protocoles d'authentification de Microsoft sont également utilisés (texte des illustrations 16 et 17 de la pièce 13).*

Le SPF Finances n'a aucun contrôle sur la manière dont Microsoft exploite ensuite ces informations de profil.

*f) Dans le cas précédent (connexion via la plateforme Sharepoint Online), il est également question, d'après le rapport d'enquête technique, [...] **de la comparaison et de la réunion d'ensembles de données par Microsoft**. Si la personne concernée se connecte via la plateforme Sharepoint avec son adresse e-mail Microsoft, Microsoft l'associe à des données que la personne concernée n'a pas fournies au SPF Finances mais aux propres données dont dispose Microsoft (le nom, le lieu et la date de naissance de la personne concernée).*

g) Il y a un cumul d'absence de transparence lors des flux de données qui se succèdent (voir les constatations du manque de transparence du SPF Finances et de Microsoft)."

130. Pour cette raison évoquée ci-dessus, le défendeur aurait donc bien dû réaliser une AIPD pour le traitement de données à caractère personnel lié aux options d'accès au service FisconetPlus avec authentification, vu les caractéristiques du traitement et vu aussi le manque de garanties spécifiques prévues par le défendeur pour protéger les données à caractère personnel des personnes concernées.

131. Plus particulièrement, de par l'utilisation de la méthode d'authentification via une entreprise tierce (les comptes utilisateur de Microsoft) qui, en tant que responsable du traitement et sans instructions concrètes du défendeur, peut relier techniquement les traitements de données à caractère personnel au moyen de comptes utilisateur via FisconetPlus avec les traitements de données à caractère personnel qui n'ont rien à voir avec le site Internet du défendeur ou les activités du défendeur, il est question de l' *"évaluation systématique et approfondie d'aspects personnels concernant des personnes physiques, qui est fondée sur un traitement automatisé"* qui est visée à l'article 35, premier alinéa, point a) du RGPD, sur laquelle se basent des décisions qui *"affectent de manière significative"* la personne physique.

132. La Chambre Contentieuse constate dès lors une infraction à l'article 34 du RGPD.

f. Le placement de cookies via FisconetPlus et la protection des données par défaut et la protection des données dès la conception (articles 4, 6, 7 et 25 du RGPD ; article 5 de la directive vie privée et communications électroniques)

133. Le Service d'Inspection est arrivé à la constatation que le défendeur considère le 'further browsing' ('poursuite de la navigation') sur les deux sites Internet comme un consentement pour l'utilisation de cookies, même si ces cookies ne sont pas nécessaires au bon fonctionnement du site Internet.

134. D'un côté, le Service d'Inspection souligne le fait que la 'poursuite de l'utilisation' n'est pas la même chose qu'un consentement donné en vertu du RGPD. D'un autre côté, le Service d'Inspection constate que la politique de cookies du défendeur présente des manquements : "*Dans la politique, il n'y a aucune différenciation entre les différents types de cookies ou traceurs. [Il est] impossible pour [la personne concernée] d'avoir l'information sur les différents cookies, mais aussi sur les cookies pour lesquels [la personne concernée] a le droit d'exprimer son consentement (Cookies non strictement nécessaires)*".³⁹ En outre, une comparaison entre les cookies énoncés dans la politique de cookies et ceux chargés lors de l'ouverture du site Internet révèle que l'énumération dans la politique de cookies n'est pas complète (exhaustive) et n'est pas entièrement correcte.

135. Le Service d'Inspection constate que le défendeur utilise différents cookies appelés 'cookies de session' (schéma 4 du rapport technique). De tels cookies de session sont 'non persistants', ce qui signifie qu'ils ne sont présents que pendant la session, c'est-à-dire tant que le navigateur est ouvert. Ils ne subsistent pas au fil des différentes sessions. Le fait qu'un cookie ne soit enregistré que temporairement n'est toutefois pas similaire au fait que ce cookie soit simplement technique et nécessaire.

136. La Chambre Contentieuse considère la problématique relative aux cookies selon les différentes possibilités d'accès à FisconetPlus. D'un côté, il y a des cookies qui sont placés par le défendeur lui-même et d'un autre côté, il y a une possibilité d'accès via Microsoft, où des cookies sont placés par Microsoft.

137. En ce qui concerne la première possibilité d'accès, le Service d'Inspection constate que treize cookies sont actifs. La Chambre Contentieuse estime que cette pratique du défendeur n'est pas

³⁹ Extrait du rapport technique rédigé en français. "*Dans la politique, il n'y a aucune différenciation entre les différents types de cookies ou traceurs. Impossible pour l'utilisateur d'avoir l'information sur les différents cookies, mais aussi sur les cookies pour lesquels il a droit d'exprimer son consentement. (Cookies non strictement nécessaires)*".

sanctionnable, étant donné qu'il manque un fondement de fait dans les constatations du Service d'Inspection quant à la nature essentielle ou non essentielle de ces cookies. C'est pourquoi la Chambre Contentieuse souhaite, *prima facie* et sur la base des moyens de défense dans les conclusions du défendeur, partir du principe que ces treize cookies sont effectivement des cookies techniquement nécessaires, et qu'ils sont par conséquent essentiels. En application de l'article 5, troisième alinéa de la directive vie privée et communications électroniques, l'exigence de consentement ne s'applique pas pour ce type de cookies.

138. La Chambre Contentieuse insiste toutefois sur l'importance d'une politique de cookies légalement correcte. Afin de fournir des informations correctes à l'utilisateur final, et atteindre ainsi par ailleurs la transparence, il ne peut pas y avoir de décalage entre les cookies énumérés dans la politique de cookies et les cookies placés en réalité, ce qui s'est révélé être le cas en l'espèce vu l'absence de mention d'un seul cookie, ce que le défendeur reconnaît aussi dans ses conclusions en réplique.

139. En ce qui concerne la deuxième possibilité d'accès (via Microsoft), la Chambre Contentieuse renvoie à la partie 3.3. de la présente décision. On y expose que le défendeur doit bel et bien être considéré comme le responsable (conjoint) du traitement avec Microsoft, pour les traitements réalisés par ce dernier sur le site Internet du défendeur, lorsque le défendeur fait usage du processus d'authentification de Microsoft. Il en va de même pour le placement de cookies et le traitement de données à caractère personnel y afférent.

140. La corrélation entre l'accès au service du défendeur et les facilités de connexion de Microsoft est en effet si forte que le défendeur est coresponsable pour les cookies qui sont placés chez l'utilisateur par Microsoft. Le défendeur a en outre opéré un choix délibéré de collaborer avec Microsoft.

141. Il ressort des constatations du Service d'Inspection⁴⁰ que Microsoft place 54 cookies chez l'utilisateur final, dont aussi des cookies qui ne sont pas purement "essentiels". L'enquête sous-jacente du Service d'Inspection est technique et détaillée (le rapport technique comporte à lui seul 42 pages) et dans la présente décision, la Chambre Contentieuse ne renvoie dès lors que dans les grandes lignes à ce qui y est constaté.

142. La Chambre Contentieuse renvoie en particulier au rapport technique dans lequel le Service d'Inspection affirme que les cookies qui sont placés lors de l'authentification avec le compte utilisateur Microsoft (aussi bien le compte utilisateur 'anonyme' que le 'normal') ne sont pas tous des cookies essentiels, et renvoie au type "ANON" et "NAP", dont l'enquête du Service d'Inspection

⁴⁰ Rapport technique, pp. 33-38.

démontre que les cookies sont utilisés pour le marketing, la personnalisation et des finalités opérationnelles de Microsoft.⁴¹ En outre, les cookies peuvent également relier au profil Microsoft toute une série de données à caractère personnel telles que l'âge, la langue, le code postal, etc.

143. La Chambre Contentieuse constate qu'il s'agit ici bel et bien de cookies qui 1) ne sont pas essentiels et 2) collectent des données à caractère personnel (et les traitent donc au sens du RGPD). L'utilisation de tels cookies est soumise à une obligation d'information (article 10 de la directive vie privée et communications électroniques et article 13 du RGPD) et de consentement donné par l'utilisateur final (article 5, troisième alinéa de la directive vie privée et communications électroniques et articles 6 et 7 *juncto* article 4, point 11 du RGPD).

144. La Chambre Contentieuse rappelle que la poursuite de l'utilisation ('further browsing') ne peut pas être assimilée à l'octroi d'un consentement valable en vertu du RGPD et de la directive vie privée et communications électroniques. Ce consentement requiert en effet, en vertu de l'article 4, point 11, de l'article 6, premier alinéa, point a) et de l'article 7 du RGPD, ainsi que sur la base de l'article 5, troisième alinéa de la directive vie privée et communications électroniques, un consentement libre, spécifique, clair, indubitable et actif.

145. Un tel consentement ne répond pas aux conditions légales lorsque la personne concernée, après avoir vu une mention sur l'utilisation de cookies sur un site Internet, poursuit son utilisation de ce site Internet.⁴² Dans la situation constatée par le Service d'Inspection où le défendeur se repose sur le 'further browsing' en lieu et place d'une bannière de cookies à part entière avec un consentement licite, la Chambre Contentieuse constate (vu l'absence de la possibilité d'un consentement valable en droit au moment de la détermination des moyens du traitement) une violation des articles 6, 7 *juncto* 4, point 11 et de l'article 25, premier alinéa du RGPD.

g. Les autres constatations du Service d'Inspection (articles 31, 38 et 39 du RGPD)

146. Le Service d'Inspection affirme notamment que le défendeur viole l'article 38 et l'article 39, en raison de "*la non-implication en temps opportun*" du DPO "*lors de l'adaptation du service*

⁴¹ Voir le rapport technique, pp. 37-38 : "Par contre, ceux déposés indirectement par la partie tierce, ne le sont pas tous. En effet, nous y trouvons entre autres les cookies « ANON » ; « NAP » ; pour lesquels nous avons la confirmation que ce sont des cookies marketing, et de tracking: ANON : Contains the ANID, a unique identifier derived from your Microsoft account, which is used for advertising, personalization, and operational purposes. It is also used to preserve your choice to opt out of interest-based advertising from Microsoft if you have chosen to associate the opt-out with your Microsoft account; NAP : Contains an encrypted version of your country, postal code, age, gender, language and occupation, if known, based on your Microsoft account profile".

⁴² Voir la décision de la Chambre contentieuse 12/2019 du 17 décembre 2019 ; Arrêt CJUE du 1^{er} octobre 2019, *Planet49 GmbH*, C-673/17, ECLI:EU:C:2019:801.

FisconetPlus" ainsi qu'en raison de l'absence de "*point de vue clairement distinct*" entre celui du DPO et celui de "*la présidence du [défendeur]*."

147. Selon la Chambre Contentieuse, les imprécisions apparues dans les réponses respectivement du défendeur et du DPO sont étroitement liées aux infractions commises par le défendeur à la lumière de l'article 5, premier alinéa, points a) et c) du RGPD. En ce sens et aux yeux de la Chambre Contentieuse, les constatations du Service d'Inspection concernant les articles 38 et 39 du RGPD ne donnent pas lieu à des infractions supplémentaires à la législation dans le chef du défendeur.

148. En ce qui concerne le respect de l'obligation de coopération reprise à l'article 31 du RGPD, la Chambre Contentieuse estime également qu'il n'y a pas d'infraction, dès lors que le défendeur affirme à juste titre que le droit de défense et l'interdiction d'auto-incrimination doivent aussi être pris en compte dans l'examen de l'obligation de coopération.⁴³ Lorsqu'un responsable du traitement fournit des informations quant à son interprétation d'une situation juridique ou de fait, et que le Service d'Inspection ou un autre organe de l'APD n'est pas d'accord, on ne peut le considérer comme une violation supplémentaire en vertu de l'article 31 du RGPD.

4. Les violations du RGPD et les requêtes du plaignant

149. La Chambre Contentieuse estime que les violations des dispositions suivantes par le défendeur sont avérées :

- a. **article 5, premier alinéa, point a), juncto article 25, premier alinéa du RGPD**, étant donné que le défendeur proposait sur son site Internet FisconetPlus deux possibilités d'accès, avec plus de fonctionnalités que la possibilité d'accès où aucune donnée à caractère personnel n'était traitée, au moyen de l'authentification via un fournisseur de services tiers, Microsoft, où des données à caractère personnel étaient traitées, ce qui, pour les raisons exposées dans la motivation qui précède, ne peut pas être considéré comme un traitement loyal et transparent de données à caractère personnel au moment de la détermination des moyens du traitement ;
- b. **article 5, premier alinéa, point c), juncto article 25, premier alinéa du RGPD**, étant donné que le défendeur proposait sur son site Internet FisconetPlus une possibilité d'accès où la personne concernée pouvait utiliser un compte utilisateur de Microsoft existant ou nouveau (un compte utilisateur non 'anonyme'), où des traitements de données à caractère personnel nécessaires pour l'authentification étaient utilisés par

⁴³ Conclusions en réplique du défendeur, point 155.

Microsoft, ce qui ne répond pas au principe de minimisation des données, au moment de la détermination des moyens du traitement ;

- c. **article 35 du RGPD**, étant donné que le défendeur aurait dû réaliser une AIPD pour l'utilisation des comptes utilisateur de Microsoft via son site Internet FisconetPlus, dès lors que l'utilisation de ce fournisseur de services tiers comportait un risque potentiellement élevé pour les droits et les libertés des personnes physiques ;
- d. **articles 6, premier alinéa et 7, juncto 4, point 11) et article 25, premier alinéa du RGPD**, étant donné que de par l'utilisation de comptes utilisateur Microsoft par le défendeur sur son site Internet FisconetPlus, des cookies non essentiels ont été placés et qu'aucun consentement valable n'a été obtenu pour ceux-ci, vu que la bannière sur le site Internet précité permettait aussi le consentement au moyen du 'further browsing', au moment de la détermination des moyens du traitement.

150. Étant donné que le défendeur a indiqué à la Chambre Contentieuse dans ses moyens de défense que, suite à la mesure provisoire du Service d'Inspection en vertu de l'article 70 de la LCA contre laquelle le défendeur n'a pas introduit de recours auprès de la Chambre Contentieuse, le site Internet ne proposait plus à ce jour une possibilité d'authentification au moyen des comptes utilisateur Microsoft, la Chambre Contentieuse n'estime pas nécessaire d'ordonner au défendeur de mettre les traitements en conformité ; la Chambre Contentieuse se contentera toutefois de réprimander le défendeur. En vertu de l'article 220, § 1, deuxième alinéa de la loi du 30 juillet 2018 *relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel*. (M.B. 5 septembre 2018), la Chambre Contentieuse n'est pas compétente pour infliger une amende au sens de l'article 83 du RGPD à des organismes publics.

151. Vu l'importance de la transparence quant au processus décisionnel de la Chambre Contentieuse, la présente décision est publiée, en vertu de l'article 100, § 1, 16° de la LCA, sur le site Internet de l'Autorité de protection des données, avec publication aussi des données d'identification directes des parties et personnes physiques en question, vu la personne du plaignant, les compétences spécifiques du défendeur et l'importance de la transparence à cet égard vis-à-vis du monde extérieur. La Chambre Contentieuse souligne, par souci d'exhaustivité, que le plaignant et le défendeur ont marqué leur accord à ce sujet (après avoir été interrogés sur la question lors de l'audition), ou du moins n'ont pas avancé d'arguments indiquant que la publication de la décision sans suppression de leurs données d'identification directes leur serait particulièrement préjudiciable.

PAR CES MOTIFS,

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

- conformément à l'**article 100, § 1, 5° de la LCA** et à l'**article 58, deuxième alinéa, point b) du RGPD**, de réprimander le défendeur en raison des violations des articles 5, premier alinéa, points a) et c) ; 6, premier alinéa ; 7 ; 25, premier alinéa et 35 du RGPD.

En vertu de l'article 108, § 1^{er} 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