



**Chambre Contentieuse**

**Décision quant au fond 103/2026 du 12 mai 2026**

**Numéro de dossier : DOS-2021-01999**

**Objet : Plainte contre Isabel SA concernant le service d'authentification et d'identification TruliUs**

La Chambre Contentieuse de l'Autorité de protection des données (ci-après « **APD** »),

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

Vu la Loi du 3 décembre 2017 *portant création de l'APD*<sup>1</sup> (ci-après « **LCA** ») ;

Vu la Loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, ci-après « **LTD** » ;

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<sup>2</sup> ;

Vu les pièces du dossier, en ce compris les conclusions des parties, ainsi que le formulaire de sanction et la réaction de la défenderesse à ce dernier ; et

Entendu les parties lors de l'audition du 15 décembre 2025;

**A pris la décision suivante concernant :**

**Le plaignant :** X, ci-après « le plaignant » ;

**La défenderesse :** Isabel SA, dont le siège social est établi à Boulevard De L'impératrice 13-15, 1000 Bruxelles, inscrite sous le numéro d'entreprise BE0455530509,

---

<sup>1</sup> L'APD rappelle que la loi organique révisée est entrée en vigueur le 01/06/2024. Elle ne s'applique qu'aux plaintes, aux dossiers de médiation, aux requêtes, aux inspections et aux procédures devant la Chambre Contentieuse initié(e)s à partir de cette date. Les dossiers initiés avant le 01/06/2024, tel que le présent dossier, sont soumis aux dispositions de l'ancienne version de la LCA accessible ici : <https://www.autoriteprotectiondonnees.be/publications/loi-organique-de-l-apd.pdf>

<sup>2</sup> Le nouveau règlement d'ordre intérieur de l'APD, consécutif aux modifications apportées par la Loi du 25 décembre 2023 modifiant la loi du 3 décembre 2017 portant création de l'autorité de protection des données (LCA) est entré en vigueur le 01/06/2024. Il ne s'applique qu'aux plaintes, aux dossiers de médiation, aux requêtes, aux inspections et aux procédures devant la Chambre Contentieuse initié(e)s à partir de cette date. Les dossiers initiés avant le 01/06/2024 sont soumis aux dispositions règlement d'ordre intérieur tel qu'il existait avant cette date.

représentée par Maître Erik VALGAEREN et Maître Cyril FISCHER, avocats dont le cabinet est sis à [...], ci-après : « la défenderesse » ou « Isabel ».

## I. Faits et procédure

1. Le 29 mars 2021, le plaignant a introduit une plainte auprès de l’Autorité de protection des données (ci-après « **APD** ») à l’encontre de la partie défenderesse.
2. Le plaignant dénonce le processus d’authentification de la solution TruliUs développé par Isabel. TruliUs est un service permettant aux entreprises de s’identifier et s’authentifier auprès d’autres entreprises qui proposent le service TruliUs sur leur plateforme digitale. En d’autres mots, à l’instar de Belgian Mobile ID (ci-après « itsme »)<sup>3</sup>, TruliUs permet à des personnes physiques d’agir de manière digitale pour le compte d’une entreprise, en assurant aux partenaires que la personne qui prétend agir pour le compte d’une entreprise est bien la personne qu’elle prétend être, et qu’elle a la capacité d’agir pour le compte de l’entreprise.
3. Le plaignant est gérant de la SRL Z (ci-après « Z » ou « sa société »). Le comptable de sa société est la SA Z1 (ci-après « Z1 » ou « le comptable »). Ce comptable utilise une plateforme numérique développée par la SRL Z2 (ci-après « Z2 » ou « la plateforme comptable » ) pour notamment permettre le dépôt de documents auprès du comptable.
4. En l’espèce, la solution TruliUs permettait à des personnes physiques, comme le plaignant, de s’identifier afin de pouvoir agir au nom et pour le compte de sa société auprès de la plateforme numérique de son comptable .
5. Le plaignant dénonce dans sa plainte les divergences entre les données mentionnées dans la déclaration de confidentialité figurant sur le site de TruliUs et les données effectivement collectées au moyen du système itsme. Il s’interroge en outre sur la pertinence de la collecte de certaines données telles que la nationalité, la photo de la carte d’identité électronique, le lieu de naissance et la date de naissance. Enfin, le plaignant indique avoir adressé deux courriels au défendeur pour exercer son droit d’accès, les 11 et 19 mars 2021, sans avoir reçu de réponse de la défenderesse.

---

<sup>3</sup> La Chambre Contentieuse précise qu’itsme (Belgian Mobile ID SA) n’est pas partie à la présente procédure et n’est mise en cause à aucun titre par la présente décision. Les mentions d’itsme dans la présente décision ont une finalité strictement descriptive du fonctionnement technique du service TruliUs. Voy. point 141 de la section IV. Publication de la décision.

| Ce qui est collecté   | Ce que Trulius annonce collecter   |
|---|--|
|  | <p>Disponible sur leur site : <a href="https://www.trulius.be/fr/declaration-de-confidentialite/">https://www.trulius.be/fr/declaration-de-confidentialite/</a></p> <p><b>2 DONNÉES QUE NOUS COLLECTONS</b></p> <p>Lorsque vous vous inscrivez sur la plateforme Trulius, nous collectons les types de données personnelles suivantes vous concernant :</p> <p>a. Données d'identification : <u>vos nom, adresse, numéro de registre national, adresse email et mot de passe</u> ;</p> <p>b. Informations sur l'entreprise pour laquelle vous travaillez : son nom et son adresse, si vous en êtes un représentant légal ou un représentant permanent et la fin de votre mandat, votre fonction au sein de l'entreprise et vos pouvoirs de signature dans l'entreprise ;</p> <p>c. Informations liées à votre utilisation des services et à leur sécurité, y compris les informations techniques des appareils utilisés pour accéder au site web et à la plateforme, les identifiants de ces appareils, votre adresse IP, les informations du système d'exploitation et du navigateur, les connexions et les activités effectuées.</p> |

Capture d'écran issue du rapport d'enquête du Service d'Inspection (page 2), présentée à titre d'illustration.

6. Le 2 septembre 2021, conformément à l'article 96, § 1er de LCA, la demande de la Chambre Contentieuse de procéder à une enquête est transmise au Service d'Inspection, de même que la plainte et l'inventaire des pièces.
7. Le 11 septembre 2023, l'enquête du Service d'Inspection est clôturée, le rapport est joint au dossier et celui-ci est transmis par l'inspecteur général au Directeur de la Chambre Contentieuse (art. 91, § 1er et § 2 de la LCA). Le rapport d'enquête comporte les constatations suivantes :
  - Constatation 1: Violation des **articles 5.1.a), 12.1 et 13 du RGPD**, en raison de l'absence d'information préalable fournie au plaignant. Les données traitées par le défendeur via Trulius sont incomplètement référencées dans la déclaration de confidentialité qui a été présentée au plaignant avant la communication de ses données à caractère personnel via itsme. Ladite déclaration de confidentialité ne reprend que les informations concernant les traitements pour lesquels le défendeur se considère comme responsable du traitement. Le plaignant a donc été confronté à une information confuse en constatant des divergences entre les informations sur le traitement de données annoncé et les données personnelles effectivement recueillies.
  - Constatation 2: Violation des **articles 5.1.a), 12.1 et 15.1 du RGPD**, en raison du non-respect par le défendeur du droit d'accès de la personne concernée par l'absence de réponse à deux e-mails en date du 11 mars 2021 et d'un rappel le 19 mars 2021.
  - Constatation 3: Violation des **articles 5.1.c) et 25.2 du RGPD**, en raison du non-respect du principe de minimisation et du manque de protection des données par défaut. En l'occurrence, le Service d'Inspection constate que plus d'une dizaine de données sont collectées afin de pouvoir créer un profil utilisateur et

de partager ce profil sans que la nécessité de la collecte de chacune des données ne soit démontrée. En collectant des données excédentaires à la finalité d'identification/authentification poursuivie, le principe de protection des données par défaut n'est pas respecté par la défenderesse.

- **Constatation 4:** Violation des **article 5.2 du RGPD**, en raison du non-respect du principe de responsabilité. Le défendeur se déresponsabilise d'un traitement dont il détermine à tout le moins les moyens. Le Service d'Inspection constate que le défendeur doit revêtir la qualité de responsable du traitement lorsqu'il fournit les services d'identification/authentification aux sociétés/indépendants sous la dénomination commerciale TruliUs et traite les données d'authentification de leurs représentants.

8. Le 22 février 2024, la Chambre Contentieuse décide, en vertu de l'article 95, § 1<sup>er</sup>, 1<sup>o</sup> et de l'article 98 de la LCA, que le dossier peut être traité sur le fond. Les parties concernées sont informées par envoi recommandé des dispositions telles que reprises à l'article 95, § 2 ainsi qu'à l'article 98 de la LCA. Elles sont également informées, en vertu de l'article 99 de la LCA, des délais pour transmettre leurs conclusions.

Au regard des pièces du dossier, la Chambre Contentieuse a invité les parties à conclure quant aux violations constatées dans le rapport d'enquête du Service d'Inspection repris ci-dessus (point 7).

9. Le 5 avril 2024, la Chambre Contentieuse reçoit les conclusions en réponse de la défenderesse. Cette dernière ayant déposé des conclusions de synthèse, son argumentaire est résumé au point 11 ci-après.

**Les conclusions du plaignant :**

10. Le 5 avril 2024, la Chambre Contentieuse reçoit une réaction du plaignant. Celui-ci réagit à certains passages des conclusions de la défenderesse comme suit :
  - En ce qui concerne l'argument de la défenderesse selon lequel le problème d'absence de réponse aux e-mails du plaignant découlerait d'une mise à jour de Microsoft (point 10 des conclusions de la défenderesse), le plaignant fait valoir que cet argument reflète le manque de compétence des équipes informatiques de la défenderesse. Le plaignant explique que, travaillant dans le domaine informatique et régulièrement avec des produits Microsoft, ce type de mise à jour est annoncé plusieurs mois à l'avance, de sorte qu'il en résulte une faute dans le chef de la défenderesse dès lors que son service informatique n'a pas pris les mesures adéquates pour éviter ce problème.
  - En ce qui concerne la remarque de la défenderesse selon laquelle le plaignant aurait envoyé « pas moins de sept emails » à l'APD remettant en question la

rapidité de traitement de sa plainte (point 12 des conclusions de la défenderesse), le plaignant fait valoir qu'il a effectivement envoyé plusieurs relances dès lors qu'en tant que plaignant, il n'a jamais été informé du suivi concret réservé à sa plainte. Il estime dès lors légitime de s'interroger sur la considération apportée à ce type de dossier et souligne que ses sept relances sont, de surcroît, suffisamment espacées dans le temps. Le plaignant exprime enfin des doutes quant à la pertinence, pour la défenderesse, de soulever cet élément, qui vise principalement à mettre en cause sa crédibilité.

- En ce qui concerne l'argument de la défenderesse selon lequel le plaignant n'aurait « même pas pris la peine d'essayer d'envoyer un courrier postal », ce qui démontrerait à suffisance que le traitement de ses données n'avait pas un fort impact sur lui (point 57 des conclusions de la défenderesse), le plaignant fait valoir qu'en 2021, s'agissant d'une société offrant un service informatique, il est pour le moins étonnant de lui reprocher de ne pas avoir recouru à un courrier postal. Il indique avoir suivi la procédure proposée, à savoir contacter la défenderesse via les coordonnées fournies, et rappelle qu'il ne lui appartient pas de pallier les défaillances des équipes de la défenderesse si celles-ci ne sont pas en mesure de maintenir leur infrastructure informatique de manière adéquate.

**Les conclusions de la défenderesse :**

11. Le 27 mai 2024, la Chambre Contentieuse reçoit les conclusions de synthèse de la part de la défenderesse. L'argumentation de la défenderesse peut être résumée comme ci-dessous :

- **Réfutation de la constatation 1 - absence d'information préalable du plaignant :**

- o À titre de **premier moyen**, la défenderesse soutient que, dans le cadre de l'activité de traitement en cause, elle agit en tant que sous-traitante et non en tant que responsable du traitement. Elle fait valoir, à cet égard, que le service TruliUs constitue un service standardisé mis à la disposition de ses clients, lesquels décident librement d'y recourir et assument ainsi la détermination des finalités et des moyens essentiels des traitements. La défenderesse estime agir en tant qu'intermédiaire entre deux entités qui souhaitent contracter ensemble et considère que la finalité d'authentification et d'identification ne sert pas ses propres intérêts, mais ceux de ses clients (en l'espèce, Z). Quant aux moyens essentiels du traitement, la défenderesse estime que ce sont ses clients qui exercent une influence déterminante sur ceux-ci, dans la mesure où (i) ils déterminent qui sont les destinataires des données, les personnes concernées et la durée du traitement et (ii) ils décident librement de faire appel au service TruliUs. En effet, l'utilisation de TruliUs n'était pas obligatoire, une

identification « classique » restant possible. La défenderesse souligne encore que les conditions générales de TruliUs prévoient expressément qu'elle agit comme sous-traitante pour le compte du client. Elle invoque en outre la cohérence de sa position, documentée de longue date dans son analyse relative à la protection des données (« AIPD »), son registre des activités de traitement et sa documentation contractuelle. En conclusion, la défenderesse soutient que Z, la société dont le plaignant est le gérant, doit être qualifiée de responsable du traitement pour le traitement en cause et qu'elle-même doit être considérée comme sous-traitante de Z.

- À titre de **deuxième moyen**, la défenderesse soutient que l'obligation d'information énoncée aux articles 5.1.a), 12.1 et 13 du RGPD incombe au responsable du traitement. Le sous-traitant n'est pas tenu au respect de cette obligation. Il doit uniquement aider le responsable du traitement à respecter son obligation d'information et ce, « dans toute la mesure du possible »
- À titre de **troisième moyen**, la défenderesse soutient que l'article 13 du RGPD ne prescrit aucune obligation d'information quant aux (catégories de) données traitées.
- À titre de **quatrième moyen**, la défenderesse soutient qu'en vertu de l'article 13.4 du RGPD, l'obligation d'information ne s'applique plus lorsque, et dans la mesure où, la personne concernée dispose déjà de ces informations.
- **Réfutation de la constatation 2 - non-respect des droits de la personne concernée :**
  - À titre de **cinquième moyen**, la défenderesse soutient que l'obligation de répondre à l'exercice des droits de la personne concernée incombe au responsable du traitement.
- **Réfutation de la constatation 3 - non-respect du principe de minimisation / manque de protection des données par défaut**
  - À titre de **sixième moyen**, la défenderesse soutient que l'obligation de minimisation des données incombe au responsable du traitement.
- **Réfutation de la constatation 4 - non-respect du principe de responsabilité**
  - À titre de **septième moyen**, la défenderesse soutient que le respect du principe de responsabilité incombe au responsable du traitement.
- À titre subsidiaire, à titre de **huitième moyen**, la défenderesse soutient que la défenderesse n'a pas commis de faute. Une erreur de qualification dans le chef de la défenderesse ne saurait être constitutive d'une faute.

- À titre subsidiaire, à titre de **neuvième moyen**, la défenderesse soutient que, compte tenu de l'impact mineur du traitement en cause et du délai qui a été laissé à la défenderesse pour répondre au plaignant, la plainte devrait être classée sans suite (le plaignant a envoyé son premier e-mail à la défenderesse en date du 11 mars 2021, et introduit une plainte en date du 29 mars 2021, soit moins d'un mois après avoir envoyé son premier e-mail).
  - À titre infiniment subsidiaire, à titre de **dixième moyen**, la défenderesse soutient que la défenderesse a coopéré avec l'APD, a agi de bonne foi et a pris un large éventail de mesures pour respecter le RGPD.
12. Le 13 avril 2026, la Chambre Contentieuse fait connaître à la défenderesse son intention de procéder à l'imposition d'une amende administrative ainsi que le montant de celle-ci, afin de donner à la défenderesse l'occasion de se défendre avant que la sanction soit effectivement infligée.
13. Le 4 mai 2026, la Chambre Contentieuse reçoit la réaction de la défenderesse concernant l'intention d'infliger une amende administrative et le montant de celle-ci. Elle a dûment pris en compte les réactions de la défenderesse lorsqu'elle a décidé du montant final de l'amende. La défenderesse fait valoir que l'erreur de qualification qui lui est reprochée ne saurait constituer une négligence grave eu égard à la complexité reconnue des notions de responsable du traitement et de sous-traitant ; qu'une telle erreur ne saurait par ailleurs constituer, en tant que telle, une violation autonome de l'article 5.2 du RGPD, sous peine de méconnaître le principe de légalité des peines ; que le montant de l'amende envisagée serait disproportionné au regard d'autres décisions précédemment rendues par la Chambre Contentieuse ; que la décision ne devrait pas être publiée, ou ne devrait l'être que de manière anonymisée ; et que la durée de la procédure serait constitutive d'une violation de l'article 6 de la Convention européenne des droits de l'homme (ci-après « **Conv. EDH** »).

## II. Motivation

### II.1. Quant à la qualification de la défenderesse en tant que responsable du traitement au regard de l'activité de traitement d'authentification et d'identification – principe de responsabilité (article 5.2 du RGPD)

14. La Chambre Contentieuse relève que, tout au long de la procédure, la défenderesse a soutenu qu'elle ne revêt pas la qualité de responsable du traitement, mais celle de sous-traitante de la société dont le plaignant est le gérant, pour ce qui est de l'activité de traitement d'authentification et d'identification mise en œuvre dans le cadre du service TruliUs (point 11). Cette activité de traitement recouvre un ensemble d'opérations consistant notamment en (i) la collecte auprès du plaignant, par l'intermédiaire du système itsme, d'un ensemble de données à caractère personnel — telles que le nom, l'adresse, le numéro de

registre national, la date et le lieu de naissance, le numéro de carte d'identité électronique, l'adresse e-mail, le sexe, la nationalité, le numéro de téléphone et la photo de la carte d'identité électronique — en vue de la création et de la mise à jour du profil de l'utilisateur au sein de TruliUs, ainsi que (ii) du partage de ce profil avec les partenaires de la défenderesse (en l'espèce, la plateforme comptable), afin de permettre au plaignant, en sa qualité de gérant de Z, de s'identifier et de s'authentifier sur cette plateforme comptable, utilisée par son comptable.

15. La défenderesse se considère, en revanche, responsable du traitement pour d'autres traitements liés au service TruliUs, à savoir la vérification du statut de représentant légal de l'utilisateur dans la Banque-Carrefour des Entreprises (BCE)<sup>4</sup>, la création de compte, la facturation de ses services, l'investigation de problèmes techniques et de sécurité, ainsi que la réalisation de statistiques de visite de son site internet<sup>5</sup>.
16. Étant donné que la qualification de la défenderesse en tant que responsable du traitement ou sous-traitante constitue la question préalable dont dépend l'ensemble de la présente affaire, la Chambre Contentieuse s'emploiera, en premier lieu, à trancher cette question. En effet, les quatre constatations du Service d'Inspection — à savoir l'absence d'information préalable du plaignant (articles 5.1.a), 12.1 et 13 du RGPD), le non-respect du droit d'accès (articles 5.1.a), 12.1 et 15.1 du RGPD), le non-respect du principe de minimisation et de la protection des données par défaut (articles 5.1.c) et 25.2 du RGPD) ainsi que le non-respect du principe de responsabilité (article 5.2 du RGPD) — portent sur des obligations qui incombent au responsable du traitement. La défenderesse fonde d'ailleurs l'essentiel de sa défense sur sa prétendue qualité de sous-traitante de la société du plaignant pour faire valoir que ces obligations ne lui sont pas opposables. Il convient dès lors de vérifier si la défenderesse doit être qualifiée de responsable du traitement pour l'activité de traitement d'authentification et d'identification susvisée, avant d'examiner, le cas échéant, les violations rapportées par le Service d'Inspection.

#### **i. Le cadre juridique applicable**

17. L'article 4.7 du RGPD définit le responsable du traitement comme « 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 ». Il s'agit d'une notion autonome, propre à la réglementation européenne en matière de protection des données, dont l'appréciation doit se faire au départ des critères qu'elle énonce : la détermination des finalités du traitement de données concerné ainsi que la détermination des moyens

---

<sup>4</sup> Procès-verbal de l'audition tenue devant la Chambre Contentieuse le 15 décembre 2025, p. 3.

<sup>5</sup> SI, rapport d'enquête, p. 5.

(essentiels)<sup>6</sup> de celui-ci. Elle doit en outre être interprétée de manière large, afin de garantir une protection effective et complète des personnes concernées<sup>7</sup>.

18. La Chambre Contentieuse rappelle également qu'est défini comme sous-traitant au sens de l'article 4.8 du RGPD, « *la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement* ».
19. Conformément aux lignes directrices 07/2020 du Comité européen de la protection des données (ci-après « **EDPB** »)<sup>8</sup> concernant les notions de responsable du traitement et de sous-traitant dans le RGPD<sup>9</sup>, la qualification de responsable du traitement repose sur une appréciation factuelle et non sur la seule qualification contractuelle retenue par les parties<sup>10</sup>. En d'autres termes, la Chambre Contentieuse n'est aucunement liée par les qualifications que les parties se sont attribuées dans un contrat (conditions générales d'utilisation) et doit procéder à un examen au regard des traitements concrètement effectués.
20. Quant à la notion de « finalités » du traitement, elle renvoie au « pourquoi » du traitement, c'est-à-dire au résultat escompté ou à l'objectif poursuivi. C'est l'entité qui décide pourquoi le traitement a lieu qui doit être considérée comme responsable du traitement. Les décisions relatives à la finalité relèvent ainsi, par principe, du responsable du traitement et ne peuvent être déléguées au sous-traitant<sup>11</sup>. Ce dernier ne peut traiter les données qu'aux fins définies par le responsable du traitement et ne saurait poursuivre ses propres finalités<sup>12</sup>.
21. Quant aux « moyens » du traitement, il convient de distinguer entre, d'une part, les moyens essentiels, qui sont intimement liés à la finalité et à la portée du traitement — à savoir le type de données traitées, les catégories de personnes concernées, la durée de conservation et les destinataires des données — et, d'autre part, les moyens non essentiels, qui concernent des aspects pratiques et techniques de la mise en œuvre du traitement, tels que le choix d'un logiciel ou d'un support matériel<sup>13</sup>. La détermination des moyens essentiels est réservée au responsable du traitement, tandis que certains moyens non essentiels peuvent être laissés au sous-traitant.

---

<sup>6</sup> EDPB, Lignes directrices 07/2020 concernant les notions de responsable du traitement et de sous-traitant dans le RGPD, Version 2.0. du 7 juillet 2021, points 39 et suivants, disponible sur : [https://www.edpb.europa.eu/system/files/2023-10/edpb\\_guidelines\\_202007\\_controllerprocessor\\_final\\_fr.pdf](https://www.edpb.europa.eu/system/files/2023-10/edpb_guidelines_202007_controllerprocessor_final_fr.pdf).

<sup>7</sup> CJUE, arrêt du 29 juillet 2019, *Fashion ID*, C-40/17, point 66 ; CJUE, arrêt du 5 juin 2018, *Wirtschaftsakademie Schleswig-Holstein*, C-210/16, point 28 ; CJUE, arrêt du 13 mai 2014, *Google Spain et Google*, C-131/12, EU:C:2014:317, point 34.

<sup>8</sup> Le Comité européen de la protection des données (EDPB), réunit les autorités de contrôle des États membres de l'Union européenne et vise à assurer une application cohérente du RGPD.

<sup>9</sup>EDPB, Lignes directrices 07/2020, *op. cit.*

<sup>10</sup> EDPB, Lignes directrices 07/2020, *op. cit.*, points 21 et 29.

<sup>11</sup> EDPB, Lignes directrices 07/2020, *op. cit.*, point 35 et 39.

<sup>12</sup> EDPB, Lignes directrices 07/2020, *op. cit.*, point 81.

<sup>13</sup> EDPB, Lignes directrices 07/2020, *op. cit.*, points 39 à 41.

22. La Chambre Contentieuse souligne que le terme « détermine » figurant à l'article 4.7 du RGPD doit être interprété en tenant compte du degré d'influence qu'une entité exerce effectivement sur les finalités et les moyens du traitement<sup>14</sup>. A cet égard, la qualité de responsable du traitement ne requiert pas un contrôle absolu sur l'ensemble des aspects du traitement et il suffit que l'entité en cause exerce une influence déterminante sur le « pourquoi » et le « comment » du traitement pour qu'elle doive être qualifiée de responsable du traitement<sup>15</sup>.

### **ii. Positions des parties**

23. La défenderesse soutient, en substance, que le service TruliUs constitue un service standardisé mis à la disposition de ses clients et que, conformément aux lignes directrices de l'EDPB précitées<sup>16</sup>, c'est le client qui choisit librement d'utiliser ce service, en accepte les conditions générales, et assume ainsi la qualité de responsable du traitement. La défenderesse estime que la finalité d'authentification et d'identification poursuivie par TruliUs n'est pas une finalité poursuivie par Isabel en tant que telle, mais celle du client, à savoir en l'espèce, la société dont le plaignant est le gérant. Quant aux moyens essentiels du traitement, la défenderesse fait valoir que ce sont les clients et utilisateurs qui les déterminent en substance, dès lors qu'ils décident à quel partenaire communiquer leurs données, qui peut agir comme utilisateur, la durée du traitement (point 11).
24. Le plaignant s'oppose à la qualification de sous-traitante revendiquée par la défenderesse. Lors de l'audition, le plaignant a fait valoir qu'il ne comprend pas comment il pourrait assumer la responsabilité de cette activité de traitement alors que ses données sont stockées et traitées par la défenderesse, via une plateforme sur laquelle il n'exerce aucune maîtrise et avec laquelle il n'entretient aucune relation contractuelle directe.

### **iii. Position du Service d'Inspection**

25. Le Service d'Inspection conclut, dans son rapport d'enquête, que la défenderesse doit être qualifiée de responsable du traitement pour l'activité de traitement d'authentification et d'identification effectuée dans le cadre du service TruliUs.
26. Le Service d'Inspection fonde sa position sur trois éléments principaux. Premièrement, il constate qu'Isabel détermine les moyens du traitement, notamment en ce que les données d'authentification collectées via itsme sont fixées unilatéralement par la défenderesse dans les conditions d'utilisation de TruliUs<sup>17</sup>. Il estime donc que la possibilité pour les partenaires de choisir les données collectées demeure « fort théorique », dès lors que ces données sont

---

<sup>14</sup> EDPB, Lignes directrices 07/2020, *op. cit.*, points 30 et 37.

<sup>15</sup> EDPB, Lignes directrices 07/2020, *op. cit.*, points 25 à 30.

<sup>16</sup> EDPB, Lignes directrices 07/2020, *op. cit.*, point 30, 62 et 110.

<sup>17</sup> SI, rapport d'enquête, p. 11.

concrètement figées par la défenderesse<sup>18</sup>. Deuxièmement, le Service d'Inspection relève que la thèse de la défenderesse, selon laquelle Z serait responsable du traitement, conduirait à ce que le plaignant, en sa qualité de gérant de Z, aurait dû se fournir à lui-même l'information concernant la pertinence des données collectées par la défenderesse et aurait dû exercer ses droits d'accès auprès de sa propre société<sup>19</sup>. Troisièmement, le Service d'Inspection relève que, par analogie avec itsme, qui agit en qualité de responsable du traitement lorsqu'elle fournit ses services d'identification et d'authentification aux particuliers, la défenderesse doit revêtir la même qualité lorsqu'elle fournit les mêmes services aux sociétés et indépendants sous la dénomination TruliUs<sup>20</sup>. D'ailleurs, la politique de confidentialité d'itsme précise explicitement que les fournisseurs de services, en l'espèce Isabel, agissent à leur tour en qualité de responsable du traitement lorsque les données leur sont communiquées via itsme<sup>21</sup>.

27. Le Service d'Inspection en déduit qu'en se qualifiant de sous-traitante alors qu'elle détermine à tout le moins les moyens du traitement, la défenderesse se désresponsabilise d'un traitement dont elle est, en réalité, responsable, ce qui constituerait une violation de l'article 5.2 du RGPD<sup>22</sup>.

#### **iv. Appréciation de la Chambre Contentieuse**

28. La Chambre Contentieuse ne peut se rallier à la position de la défenderesse. Elle considère, sur la base de l'ensemble des éléments du dossier, que la défenderesse doit être qualifiée de responsable du traitement pour les activités de traitement d'authentification et d'identification effectuées dans le cadre du service TruliUs, et ce pour les motifs exposés ci-après.

##### **a. Quant à la détermination de la finalité**

29. La Chambre Contentieuse rappelle que la question déterminante est de savoir qui a décidé que le traitement aurait lieu et dans quel but<sup>23</sup>. En l'espèce, c'est la défenderesse qui a conçu, développé et mis sur le marché le service TruliUs en octobre 2020. La finalité de ces activités de traitement est d'offrir une solution d'identification et d'authentification de personnes physiques agissant pour le compte d'entreprises. Cette finalité a été définie unilatéralement par la défenderesse elle-même, préalablement à toute utilisation par un quelconque client.

---

<sup>18</sup> *Ibid.*

<sup>19</sup> SI, rapport d'enquête, p. 31.

<sup>20</sup> *Ibid.*

<sup>21</sup> SI, rapport d'enquête, p. 32.

<sup>22</sup> SI, rapport d'enquête, p. 39.

<sup>23</sup> EDPB, Lignes directrices 07/2020, *op. cit.*, points 32 à 38.

30. La Chambre Contentieuse rappelle que le RGPD retient une conception large de la notion de responsable du traitement, dans le but d'assurer une protection efficace et complète des personnes concernées. Dans son arrêt IAB Europe, la Cour a jugé qu'une entité doit être qualifiée de responsable du traitement dès lors qu'elle **influe**, à des fins qui lui sont propres, sur le traitement de données à caractère personnel et **participe** à la détermination des finalités et des moyens de ce traitement<sup>24</sup>. Or l'influence concrète d'Isabel SA sur le traitement litigieux est manifeste. C'est elle qui a conçu le service TruliUs, codifié les conditions de l'authentification, sélectionné les données collectés via itsme, défini les modalités d'intégration des partenaires et structuré l'ensemble du flux d'authentification. À l'instar de la situation analysée dans l'arrêt IAB Europe, la défenderesse exerce ainsi une influence déterminante sur les opérations de traitement réalisées au sein du système TruliUs. Cela suffit à fonder sa qualification de responsable du traitement, indépendamment de la question de savoir si elle accède elle-même à l'ensemble des données traitées, ce qui est, en l'espèce, en outre le cas.
31. La défenderesse soutient que la finalité d'authentification et d'identification n'est pas une finalité qu'elle poursuit en tant que telle, mais celle du client, dès lors que c'est le client, en l'espèce Z, la société dont le plaignant est le gérant, qui souhaite que ses représentants puissent s'identifier et s'authentifier. La Chambre Contentieuse ne peut se rallier à cette analyse. Il convient de distinguer l'entité qui décide du pourquoi du traitement de celle qui en tire un avantage pratique. Or, en l'espèce, c'est la défenderesse (et non Z) qui a déterminé les conditions dans lesquelles la finalité d'authentification et d'identification serait poursuivie. Ni Z, ni *a fortiori* le plaignant, n'ont joué de rôle dans sa conception. Le plaignant s'est limité à utiliser un service dont la finalité et les paramètres étaient entièrement prédéfinis. La circonstance que Z tire un avantage pratique de cette authentification, à savoir pouvoir accéder à la plateforme comptable, ne saurait suffire à en faire le responsable du traitement.
32. La défenderesse a, par ailleurs, confirmé qu'elle se considérait elle-même responsable du traitement pour plusieurs finalités liées au service TruliUs : vérification du statut de représentant légal via la BCE, création du compte, etc. Elle distingue ainsi entre les opérations pour lesquelles elle se reconnaît responsable du traitement et la seule opération d'authentification et d'identification, pour laquelle elle se déclare sous-traitante (voy point 15 ci-dessus). La Chambre Contentieuse considère qu'une telle distinction ne peut être admise. Ces activités de traitements forment en réalité un ensemble fonctionnellement indissociable, dont les différentes opérations participent d'une finalité commune et procèdent d'une architecture technique unique conçue par la défenderesse : (i) collecte des

---

<sup>24</sup> CJUE, arrêt du 7 mars 2024, IAB Europe, C-604/22, point 61. Voy. également les points 54 et 55 de l'arrêt, lesquels rappellent que la notion de « responsable du traitement » doit recevoir une définition large afin d'assurer une protection efficace et complète des personnes concernées ; CJUE, arrêt du 5 décembre 2023, CNSP, C-683/21, point 30.

données d'identification via itsme ; (ii) vérification du statut de représentant légal ; (iii) création du profil utilisateur ; (iv) partage de ce profil avec les partenaires intégrateurs. Il s'agit là d'autant d'opérations qui concourent à une seule et même finalité, permettre l'authentification et l'identification d'utilisateurs agissant pour le compte d'entreprises. Si la jurisprudence de la CJUE invite à apprécier la qualification opération par opération<sup>25</sup>, encore faut-il que les opérations en cause puissent être véritablement isolées les unes des autres. Tel n'est pas le cas en l'espèce. Scinder artificiellement les opérations composant le service TruliUs, en attribuant à la défenderesse la qualité de responsable du traitement pour certaines et celle de sous-traitante pour d'autres, aboutirait à fragmenter la responsabilité d'une activité unique. Une telle fragmentation priverait les personnes concernées de la protection efficace et complète que le RGPD entend leur garantir et l'utilisateur du service ne saurait identifier l'entité auprès de laquelle exercer ses droits selon l'opération en cause, sans même nécessairement savoir laquelle de ces opérations est concernée. Il ne saurait être admis qu'une telle dissection technique du traitement vienne affaiblir le niveau de protection assuré par le RGPD. L'ensemble de ces opérations poursuit ainsi une finalité commune, celle de permettre l'authentification et l'identification d'utilisateurs agissant pour le compte d'entreprises, et la défenderesse en détermine, pour chacune d'elles, les finalités et les moyens essentiels (comme il sera examiné ci-après).

#### ***b. Quant à la détermination des moyens essentiels***

33. La Chambre Contentieuse constate que la défenderesse a, en outre, déterminé les moyens essentiels du traitement en cause. En effet, c'est la défenderesse qui a défini unilatéralement l'ensemble des paramètres structurants du traitement, à savoir les catégories de données collectées, les catégories de personnes concernées, la durée de conservation, les destinataires et l'architecture technique du service, sans qu'aucune marge de manœuvre effective ne soit laissée au client ou à l'utilisateur.
34. S'agissant, premièrement, des **catégories de données traitées**, c'est la défenderesse qui a défini unilatéralement les données collectées via itsme dans le cadre du processus d'inscription à TruliUs. Ces données étaient figées dans les conditions d'utilisation standard de TruliUs, rédigées par la défenderesse, sans que le client ou l'utilisateur n'ait la possibilité d'en modifier l'étendue. Comme l'a relevé à juste titre le Service d'Inspection, les explications de la défenderesse quant à la possibilité pour les partenaires de paramétrer les données collectées demeurent donc « fort théoriques »<sup>26</sup>. Ce constat est renforcé par le fait qu'un grand nombre de données collectées par TruliUs via itsme n'étaient pas demandées par la plateforme comptable et ont été déterminées exclusivement par la défenderesse

---

<sup>25</sup> CJUE, arrêt du 29 juillet 2019, Fashion ID, C-40/17.

<sup>26</sup> SI, rapport d'enquête, p. 11.

(point 72). La défenderesse a d'ailleurs confirmé lors de l'audition qu'elle avait effectivement elle-même déterminé, au niveau de la conception du service, les données qu'elle jugeait nécessaires pour l'authentification et l'identification d'un utilisateur.

35. S'agissant, deuxièmement, des **catégories de personnes concernées**, si la défenderesse fait valoir que les administrateurs de Z déterminent quels utilisateurs peuvent représenter la société, la Chambre Contentieuse relève que c'est la défenderesse qui a défini les catégories de personnes concernées dans ses conditions d'utilisation, ainsi que le processus de vérification du statut de représentant légal via la BCE et le registre UBO<sup>27</sup>. Z n'a exercé aucune influence sur la définition de ces catégories.
36. S'agissant, troisièmement, de la **durée de conservation des données**, il résulte des conditions d'utilisation que la défenderesse a notamment fixé unilatéralement une durée de suppression des comptes en attente de 13 mois<sup>28</sup>. L'argument de la défenderesse selon lequel l'utilisateur déterminerait la durée du traitement dès lors qu'il peut retirer son consentement au partage à tout moment, ne peut être suivi. Le retrait du consentement ne met fin qu'à la transmission des données avec le partenaire et n'influence en rien la durée de conservation des données par la défenderesse, laquelle reste régie par les paramètres unilatéralement fixés dans ses conditions d'utilisation. La possibilité pour un utilisateur de mettre fin à une relation de service ne peut être assimilée à la détermination d'un moyen essentiel du traitement.
37. S'agissant, quatrièmement, des **destinataires des données**, c'est la défenderesse qui a contracté avec la plateforme comptable. Cette plateforme était au moment des faits, de surcroît, une filiale du groupe Isabel et le seul partenaire ayant intégré le service TruliUs. La défenderesse a ainsi déterminé en amont le cadre des destinataires potentiels des données d'authentification. La circonstance que l'utilisateur doive, dans un cas concret, se connecter pour que ses données soient effectivement partagées ne modifie pas le fait que les destinataires possibles ont été définis par la défenderesse. Le choix offert à l'utilisateur se limitait, en pratique, à accepter ou refuser le transfert vers un destinataire préalablement déterminé par la défenderesse, ce qui ne saurait être assimilé à une détermination de ce moyen par l'utilisateur.
38. En ce qui concerne, enfin, **l'architecture globale du service et les flux de données**, la Chambre Contentieuse constate que la défenderesse a conçu l'intégralité du service TruliUs: le recours à itsme comme fournisseur de vérification d'identité, le processus d'inscription et d'authentification, les modalités de vérification du statut de représentant légal, le mécanisme de partage de profils avec les partenaires. Ces éléments relèvent de

---

<sup>27</sup> Conclusions de synthèse de la défenderesse du 27 mai 2024, point 6 ; SI, rapport d'enquête, p. 18.

<sup>28</sup> SI, rapport d'enquête, p. 19 (pièce 31, réponse 6).

moyens essentiels du traitement et ont été déterminés par la seule défenderesse, sans aucune intervention du plaignant ni de sa société.

**c. Quant à l'argument tiré du service standardisé**

39. La défenderesse soutient que TruliUs constitue un service standardisé mis à la disposition de ses clients, lesquels assument la qualité de responsable du traitement en choisissant librement d'y recourir. Elle invoque, à cet égard, l'analogie avec un service de stockage dans le cloud, tant dans ses conclusions que lors de l'audition, en faisant référence aux lignes directrices de l'EDPB.
40. La Chambre Contentieuse estime que cette analogie n'est pas transposable en l'espèce. Dans l'exemple du service standardisé de stockage cloud retenu par l'EDPB dans ses lignes directrices 07/2020<sup>29</sup>, le fournisseur de services cloud met à disposition une infrastructure technique neutre (un espace de stockage) sans déterminer ni le contenu des données qui y sont déposées, ni la finalité pour laquelle elles sont traitées, ni les catégories de personnes concernées, ni la durée de conservation. C'est le client qui prend l'ensemble de ces décisions de manière autonome. Il choisit quelles données stocker et pourquoi, combien de temps les conserver et qui peut y accéder. Le fournisseur de cloud ne traite pas les données à ses propres fins et les conserve uniquement pour le compte de ses clients et selon leurs instructions, raison pour laquelle il est qualifié de sous-traitant. En l'espèce, la situation est fondamentalement différente. La défenderesse ne se contentait pas de fournir une infrastructure technique dans laquelle le client aurait librement organisé le traitement de ses données. Au contraire, c'est la défenderesse qui a conçu le service TruliUs, défini sa finalité d'authentification et d'identification, déterminé unilatéralement les catégories de données collectées via itsme, fixé les catégories de personnes concernées, établi la durée de conservation et désigné les destinataires des données. Le plaignant s'est borné à utiliser un service dont les modalités étaient entièrement prédéfinies par la défenderesse. Une telle implication suffit déjà, en soi, à fonder la qualification de responsable du traitement. Elle s'impose d'autant plus fermement au regard de l'arrêt *IAB Europe* de la CJUE, dans lequel la Cour a reconnu cette qualité à une organisation dont le rôle se limitait à élaborer des règles internes encadrant un système de partage de préférences publicitaires<sup>30</sup>. Si l'élaboration et le contrôle d'une chaîne de règles suffisent à qualifier de responsable du traitement l'entité qui en est à l'origine, à plus forte raison cette qualité doit-elle être reconnue à un acteur dont le rôle est, comme en l'espèce, considérablement plus déterminant et plus intégré.

---

<sup>29</sup> EDPB, Lignes directrices 07/2020, *op. cit.*, point 30, Exemple : service standardisé de stockage en nuage.

<sup>30</sup> CJUE, arrêt du 7 mars 2024, *IAB Europe*, C-604/22. La Cour y a notamment jugé que l'élaboration et le contrôle d'une chaîne de règles, comme le « Transparency and Consent Framework », suffisent à qualifier l'entité qui en est à l'origine de responsable du traitement.

41. À supposer même qu'il s'agisse d'un véritable service standardisé, l'EDPB subordonne la qualification de sous-traitant du fournisseur à la condition que le client reçoive une description détaillée du service et prenne la décision finale d'approuver activement la manière dont le traitement est effectué<sup>31</sup>. Or, comme il sera examiné ci-après, cette condition n'est pas non plus remplie étant donné que le plaignant n'a reçu, au moment de la collecte de ses données via itsme, aucune description complète du traitement (points 44 à 54). Ni le plaignant ni sa société n'ont donc été en mesure d'exercer un contrôle éclairé sur les modalités du traitement avant son initiation.

La Chambre Contentieuse souligne enfin que la thèse de la défenderesse conduit à des résultats manifestement absurdes, comme l'ont relevé tant le Service d'Inspection que le plaignant. Si Z devait être qualifiée de responsable du traitement, le plaignant (en sa qualité de gérant de Z) aurait dû se fournir à lui-même l'information relative aux données collectées par la défenderesse pour l'authentifier, et aurait dû exercer son droit d'accès auprès de sa propre société pour obtenir des informations détenues par un tiers avec lequel il n'a aucune relation directe. Comme l'a souligné le plaignant lors de l'audition, il est difficilement concevable qu'un utilisateur final puisse être considéré comme responsable d'un traitement réalisé par un prestataire sur lequel il n'exerce, en pratique, aucune maîtrise.

**d. Conclusion quant à la qualification et au respect de l'article 5.2 du RGPD**

42. Au vu de l'ensemble des éléments qui précèdent, la Chambre Contentieuse conclut que la défenderesse revêt la qualité de responsable du traitement au sens de l'article 4.7 du RGPD pour l'activité de traitement d'authentification et d'identification effectuée dans le cadre du service TruliUs. Comme il a été démontré ci-avant, la défenderesse a, en effet, exercé une influence déterminante tant sur les finalités que sur les moyens essentiels de ce traitement.
43. Partant, la défenderesse ne saurait se prévaloir de la qualité de sous-traitante pour se soustraire aux obligations que le RGPD impose au responsable du traitement. En se qualifiant de sous-traitante pour le traitement au cœur du litige alors qu'elle en détermine tant les finalités que les moyens essentiels, la défenderesse a manqué au principe de responsabilité consacré à l'article 5.2 du RGPD, en vertu duquel le responsable du traitement est tenu de respecter l'ensemble des principes énoncés à l'article 5.1 du RGPD et doit être en mesure de démontrer cette conformité. **La Chambre Contentieuse estime que la défenderesse a dès lors violé l'article 5.2 du RGPD.**

---

<sup>31</sup> EDPB, Lignes directrices 07/2020, *op. cit.*, point 30.

## **II.2. Quant à l'absence d'information préalable ( articles 5.1.a), 12.1 et 13 du RGPD)**

### **i. Principes généraux applicables**

44. L'article 5.1.a) du RGPD consacre, entre autres, le principe de transparence. Ce principe est concrétisé, en matière de collecte directe de données, par l'article 13 du RGPD, qui énumère les informations que le responsable du traitement est tenu de fournir à la personne concernée au moment où les données sont obtenues. Ces informations comprennent notamment l'identité et les coordonnées du responsable du traitement, les finalités du traitement, la base juridique du traitement, les destinataires des données, la durée de conservation ainsi que l'existence des droits de la personne concernée<sup>32</sup>.
45. L'article 12.1 du RGPD précise les modalités selon lesquelles cette information doit être fournie : le responsable du traitement doit prendre « *des mesures appropriées pour fournir toute information visée aux articles 13 et 14 [...] en ce qui concerne le traitement à la personne concernée d'une façon concise, transparente, compréhensible et aisément accessible, en des termes clairs et simples* ». La transparence exige que l'information soit aisément accessible et fournie de manière proactive, sans que la personne concernée n'ait à la rechercher<sup>33</sup>.

### **ii. Positions des parties**

46. La défenderesse soulève trois moyens à cet égard. En premier lieu, elle soutient que, n'étant pas responsable du traitement pour l'activité de traitement d'authentification et d'identification, l'obligation d'information découlant des articles 5.1.a), 12.1 et 13 du RGPD ne lui incombe pas (deuxième moyen)<sup>34</sup>. En deuxième lieu, elle fait valoir que l'article 13 du RGPD ne contient aucune obligation d'informer la personne concernée des catégories de données traitées, s'agissant d'une collecte directe (troisième moyen)<sup>35</sup>. En troisième lieu, elle invoque l'article 13.4 du RGPD, selon lequel l'obligation d'information ne s'applique plus lorsque la personne concernée dispose déjà de ces informations, estimant que le plaignant avait reçu les conditions générales de TruliUs lors de la création de son compte le 19 janvier 2021 (quatrième moyen)<sup>36</sup>.
47. Le plaignant fait valoir qu'il a été confronté à une information confuse, constatant des divergences significatives entre les données mentionnées dans la déclaration de confidentialité figurant sur le site de TruliUs et les données effectivement collectées au

---

<sup>32</sup> Art. 13.1 du RGPD.

<sup>33</sup> Groupe de travail « Article 29 », ancêtre de l'EDPB, Lignes directrices sur la transparence au titre du règlement 2016/679 (WP260 rév.01), adoptées le 11 avril 2018, point 11.

<sup>34</sup> Conclusions de synthèse de la défenderesse du 27 mai 2024, points 26 à 27.

<sup>35</sup> Conclusions de synthèse de la défenderesse du 27 mai 2024, points 26 à 37.

<sup>36</sup> Conclusions de synthèse de la défenderesse du 27 mai 2024, points 32 à 37.

moyen du système itsme. Le plaignant relève qu'il ne lui était pas possible, au moment de la collecte, de comprendre pourquoi la défenderesse avait besoin de données telles que sa nationalité, sa photo de carte d'identité, son lieu et sa date de naissance.

### **iii. Position du Service d'Inspection**

48. Le Service d'Inspection constate que la déclaration de confidentialité figurant sur le site de TruliUs ne reprend que les traitements pour lesquels la défenderesse se considère comme responsable du traitement et ne mentionne pas le traitement d'authentification et d'identification pour lequel elle se qualifie de sous-traitante<sup>37</sup>. Il relève ainsi un décalage entre, d'une part, les données effectivement collectées via itsme, telles que la date et le lieu de naissance, le numéro de carte d'identité eID, la nationalité, le numéro de téléphone et la photo de la carte d'identité, et d'autre part, les données mentionnées dans la déclaration de confidentialité.
49. Le Service d'Inspection constate en outre que les conditions d'utilisation de TruliUs, seul document reprenant les données effectivement collectées, ne sont pas présentées à l'utilisateur avant la communication de ses données via itsme, mais uniquement à l'étape suivante du processus d'inscription, et exclusivement en langue anglaise<sup>38</sup>. La DPO d'Isabel a elle-même reconnu pendant l'enquête que les seules informations fournies au plaignant concernant les données traitées dans le cadre du processus d'authentification sur TruliUs étaient les informations inadéquates de la déclaration de confidentialité<sup>39</sup>. Le Service d'Inspection en déduit une violation des articles 5.1.a), 12.1 et 13 du RGPD.

### **iv. Appréciation de la Chambre Contentieuse**

50. Ayant établi, aux points 14 à 43 ci-dessus, que la défenderesse revêt la qualité de responsable du traitement pour l'activité de traitement d'authentification et d'identification mise en œuvre dans le cadre du service TruliUs, la Chambre Contentieuse rejette donc le deuxième moyen de la défenderesse selon lequel l'obligation d'information ne lui serait pas opposable. En tant que responsable du traitement, la défenderesse était tenue de fournir au plaignant les informations visées à l'article 13 du RGPD, de manière transparente et accessible conformément à l'article 5.1.a) et 12.1 du RGPD.
51. En ce qui concerne le troisième moyen, selon lequel l'article 13 du RGPD ne prescrirait aucune obligation d'information quant aux catégories de données traitées, la Chambre Contentieuse relève que si l'article 13 n'impose pas expressément de communiquer la liste des catégories de données, le principe général de transparence consacré à l'article 5.1.a) du RGPD et les exigences de l'article 12.1 du RGPD imposent que la personne concernée soit en

---

<sup>37</sup> SI, rapport d'enquête, p. 32 à 34.

<sup>38</sup> SI, rapport d'enquête, p. 30.

<sup>39</sup> SI, rapport d'enquête, p. 34.

mesure de comprendre la portée concrète du traitement de ses données. En l'espèce, l'information fournie était non seulement incomplète mais également trompeuse, dès lors que la déclaration de confidentialité mentionnait certaines données d'identification tout en omettant un nombre significatif de données effectivement collectées via itsme. Le plaignant a ainsi été confronté à une information confuse, en contradiction avec le principe de loyauté et de transparence.

52. En ce qui concerne le quatrième moyen, tiré de l'article 13.4 du RGPD, la Chambre Contentieuse constate que cette exception ne peut s'appliquer en l'espèce. En effet, il résulte du rapport d'enquête que les conditions générales de TruliUs (seul document reprenant les données effectivement collectées) ne sont pas présentées à l'utilisateur avant la collecte de ses données via itsme<sup>40</sup>. Les données de l'utilisateur étaient collectées dès la connexion avec itsme sur la page de création de compte, et ce n'est qu'à l'étape suivante que les conditions générales étaient soumises à l'acceptation de l'utilisateur. Partant, le plaignant ne disposait pas des informations relatives au traitement au moment de la collecte de ses données lors de la création de son compte TruliUs, de sorte que l'exception de l'article 13.4 du RGPD n'est pas applicable.
53. La Chambre Contentieuse constate que les seules informations dont le plaignant disposait au moment de la collecte de ses données via itsme étaient celles figurant dans la déclaration de confidentialité publiée sur le site de TruliUs. Or, cette déclaration était non seulement incomplète — en ce qu'elle ne couvrait pas le traitement d'authentification et d'identification pour lequel la défenderesse se qualifiait de sous-traitante — mais également de nature à induire le plaignant en erreur quant à la portée réelle du traitement de ses données. La DPO de la défenderesse a d'ailleurs elle-même reconnu le caractère inadéquat de cette information<sup>41</sup>. La défenderesse ne communiquait une description plus complète des données collectées qu'une fois les données déjà collectées, à l'étape suivante du processus d'inscription, dans les conditions générales, rédigées exclusivement en langue anglaise.
54. La Chambre Contentieuse conclut que la défenderesse a violé les articles 5.1.a), 12.1 et 13 du RGPD en ne fournissant pas au plaignant, au moment de la collecte de ses données à caractère personnel, une information complète, transparente et aisément accessible sur le traitement de ses données dans le cadre du service TruliUs.

---

<sup>40</sup> SI, rapport d'enquête, p. 8 (étape 5), 13 à 14 (étape 10) et 30.

<sup>41</sup> SI, rapport d'enquête, p. 34.

### **II.3. Quant à l'absence de réponse au droit d'accès ( articles 5.1.a), 12.1 et 15.1 du RGPD)**

#### ***i. Principes généraux applicables***

55. Aux termes de l'article 15.1 du RGPD, la personne concernée a le droit d'obtenir du responsable de traitement la confirmation que des données à caractère personnel la concernant sont ou ne sont pas traitées. Lorsque c'est le cas, la personne concernée a le droit d'obtenir l'accès aux dites données à caractère personnel ainsi qu'à une série d'informations listées à l'article 15.1 a) à h) telles que la finalité du traitement de ses données, les destinataires éventuels de ses données ainsi que des informations relatives à l'existence de ses droits, dont celui de demander la rectification ou l'effacement de ses données ou encore celui de déposer plainte auprès de l'APD.
56. La Chambre Contentieuse rappelle, comme elle a pu le faire par le passé<sup>42</sup>, que le droit d'accès est une des exigences essentielles du droit à la protection des données, puisqu'il constitue la « porte d'entrée » qui permet l'exercice des autres droits que le RGPD confère à la personne concernée.

#### ***ii. Positions des parties***

57. La défenderesse soutient, à titre de cinquième moyen, que l'obligation de répondre à l'exercice des droits de la personne concernée incombe au responsable du traitement, et que, n'étant selon elle que sous-traitante, cette obligation ne lui est pas opposable<sup>43</sup>. Sur le plan factuel, la défenderesse explique que l'absence de réponse aux courriels du plaignant n'est pas due à une erreur humaine, contrairement à ce qu'avait initialement indiqué son premier DPO, mais à une mise à jour de Microsoft qui a interrompu le transfert des courriels reçus à l'adresse du DPO (privacy@isabelgroup.eu) vers l'adresse Isabel Customer Care, tout en continuant à les supprimer de la boîte de réception du DPO en application d'une règle Outlook configurée par la défenderesse<sup>44</sup>.
58. Le plaignant fait valoir que cet argument témoigne du manque de compétence des équipes informatiques de la défenderesse, dès lors que ce type de mise à jour Microsoft est annoncé plusieurs mois à l'avance<sup>45</sup>. Il relève qu'il a envoyé son premier courriel au DPO le 11 mars 2021 et un rappel le 19 mars 2021, sans jamais recevoir de réponse, et qu'il a suivi la procédure indiquée dans la déclaration de confidentialité de TruliUs pour contacter le DPO.

---

<sup>42</sup> Chambre Contentieuse, décision quant au fond 15/2021 du 9 février 2021 ; décision quant au fond 72/2021 du 14 juin 2021 ; décision quant au fond 27/2023 du 13 mars 2023.

<sup>43</sup> Conclusions de synthèse de la défenderesse du 27 mai 2024, points 39 à 40.

<sup>44</sup> Conclusions de synthèse de la défenderesse du 27 mai 2024, point 10.

<sup>45</sup> Courriel du plaignant du 5 avril 2024.

### iii. Position du Service d'Inspection

59. Le Service d'Inspection constate que le plaignant a adressé deux courriels au DPO de la défenderesse, les 11 et 19 mars 2021, à l'adresse e-mail de contact renseignée dans la déclaration de confidentialité de TruliUs, sans recevoir de réponse<sup>46</sup>. Le Service d'Inspection relève que si une erreur de traitement peut être admise pour un premier courriel, le fait que le rappel envoyé huit jours plus tard ait subi le même sort paraît difficilement imputable à une nouvelle erreur humaine. Le DPO de la défenderesse a d'ailleurs lui-même reconnu un problème dans le processus de traitement des demandes des personnes concernées<sup>47</sup>. Le Service d'Inspection en déduit une violation des articles 5.1.a), 12.1 et 15.1 du RGPD.

### iv. Appréciation de la Chambre Contentieuse

60. Ayant établi que la défenderesse revêt la qualité de responsable du traitement pour le traitement en cause, la Chambre Contentieuse rejette le cinquième moyen de la défenderesse selon lequel l'obligation de répondre aux demandes d'exercice des droits ne lui incomberait pas. En tant que responsable du traitement, la défenderesse était tenue, en vertu des articles 12.1 et 15 du RGPD, de répondre aux demandes d'accès du plaignant dans un délai d'un mois.
61. En l'espèce, il est établi que le plaignant a adressé deux courriels au DPO de la défenderesse, les 11 et 19 mars 2021, à l'adresse e-mail de contact indiquée dans la déclaration de confidentialité de TruliUs. La défenderesse n'a apporté aucune réponse à ces demandes.
62. La Chambre Contentieuse constate que l'explication technique avancée par la défenderesse, à savoir une mise à jour de Microsoft ayant interrompu le transfert des courriels du DPO vers la défenderesse, n'est pas de nature à exonérer la défenderesse de sa responsabilité. Il incombe en effet au responsable du traitement de mettre en place les mesures techniques et organisationnelles nécessaires pour garantir que les demandes des personnes concernées soient effectivement reçues et traitées dans les délais impartis par le RGPD. La configuration d'une règle Outlook entraînant la suppression automatique des courriels reçus à l'adresse du DPO, combinée à l'absence de tout mécanisme de vérification ou de redondance, témoigne d'un défaut dans les mesures organisationnelles mises en place par la défenderesse pour garantir le respect des droits des personnes concernées.
63. La Chambre Contentieuse relève en outre que le DPO de la défenderesse a d'ailleurs reconnu un problème structurel dans le processus de traitement des demandes des personnes concernées, en indiquant avoir pris des mesures correctives pour éviter qu'une telle situation ne se reproduise.

---

<sup>46</sup> SI, rapport d'enquête, p. 34 à 35.

<sup>47</sup> SI, rapport d'enquête, p. 7 (étape 4 - pièce 19).

64. La Chambre Contentieuse conclut que la défenderesse a violé les articles 5.1.a), 12.1 et 15.1 du RGPD en ne répondant pas aux demandes d'accès que le plaignant lui a adressées les 11 et 19 mars 2021.

**II.4. Quant à la collecte de données excédentaires - violation du principe de minimisation et de la protection des données par défaut ( articles 5.1.c) et 25.2 du RGPD)**

**i. Principes généraux applicables**

65. L'article 5.1.c) du RGPD consacre le principe de minimisation des données, selon lequel les données à caractère personnel doivent être « *adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées* ». Ce principe impose au responsable du traitement de limiter la collecte aux seules données strictement nécessaires à la réalisation de la finalité poursuivie.
66. L'article 25.2 du RGPD complète ce principe en imposant au responsable du traitement de mettre 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.

**ii. Positions des parties**

67. La défenderesse soutient, à titre de sixième moyen, que l'obligation de minimisation des données incombe au responsable du traitement et que, n'étant selon elle que sous-traitante, elle ne saurait être tenue responsable de la violation des articles 5.1.c) et 25.2 du RGPD<sup>48</sup>. A l'audition, la défenderesse a fait valoir que lors de la conception abstraite du service, les données collectées avaient été jugées nécessaires en vue de la finalité d'authentification et d'identification poursuivie par la solution TruliUs.
68. Le plaignant a contesté, tant dans sa plainte initiale que lors de l'audition, la nécessité de la collecte de nombreuses données telles que la nationalité, la photo de la carte d'identité, le lieu de naissance et la date de naissance. Il a fait observer que, par comparaison, lorsqu'il s'authentifie sur des plateformes gouvernementales, les données collectées se limitent au numéro de registre national, à l'adresse e-mail, au nom et au prénom, et que ces plateformes n'ont pas besoin de davantage pour l'identifier. Le plaignant a également relevé que la photo collectée n'était pertinente que si elle était comparée à une autre image, ce qui ne pouvait pas être le cas en l'espèce.

---

<sup>48</sup> Conclusions de synthèse de la défenderesse du 27 mai 2024, points 41 à 45.

### iii. Position du Service d'Inspection

69. Le Service d'Inspection constate que plus d'une dizaine de données sont collectées dans le cadre du processus d'inscription à TruliUs afin de créer un profil utilisateur et de partager ce profil, sans que la nécessité de chacune de ces données ne soit démontrée<sup>49</sup>. Le Service d'Inspection relève en particulier que la plateforme comptable, seul partenaire à avoir intégré le service TruliUs, ne requérait que le prénom, le nom, la langue et l'e-mail de l'utilisateur, ainsi qu'un token de validation de l'authentification<sup>50</sup>. Le Service d'Inspection émet des doutes quant à la nécessité de collecter, à chaque connexion, en plus des autres données déjà collectées, des données telles que la nationalité, le sexe, l'adresse e-mail et le numéro de téléphone de l'utilisateur.
70. Le Service d'Inspection relève en outre que la DPO de la défenderesse a reconnu que le numéro de carte d'identité eID a été collecté sans être nécessaire, en raison d'une erreur de paramétrage technique<sup>51</sup>. Cette donnée figurait dans la liste des données collectées auprès du plaignant. Le Service d'Inspection en déduit qu'en collectant des données excédentaires à la finalité d'identification et d'authentification poursuivie, la défenderesse a enfreint les articles 5.1.c) et 25.2 du RGPD.

### iv. Appréciation de la Chambre Contentieuse

71. Ayant établi que la défenderesse revêt la qualité de responsable du traitement, la Chambre Contentieuse rejette le sixième moyen de la défenderesse selon lequel l'obligation de minimisation des données ne lui serait pas opposable.
72. La Chambre Contentieuse constate que la défenderesse collecte, dans le cadre du processus d'inscription à TruliUs, un nombre de données manifestement excédentaire au regard de la finalité d'authentification et d'identification poursuivie. En effet, ces données étaient censées permettre l'identification/authentification de l'utilisateur auprès de la plateforme comptable. Or, pour procéder à l'authentification, la plateforme comptable ne requérait que le prénom, le nom, la langue, l'adresse e-mail ainsi qu'un token de validation. La défenderesse a toutefois collecté, en plus de ces données, la nationalité, le sexe, le numéro de téléphone, la date et le lieu de naissance, le numéro de carte d'identité eID, le numéro de registre national et la photo de la carte d'identité électronique. La défenderesse n'a pas démontré en quoi chacune de ces données additionnelles était nécessaire au regard de la finalité spécifique d'authentification et d'identification. La défenderesse justifie la collecte de ces données par la nécessité pour les « administrateurs » de valider l'identité d'un

---

<sup>49</sup> SI, rapport d'enquête, p. 35 à 38.

<sup>50</sup> SI, rapport d'enquête, p. 23 à 24.

<sup>51</sup> SI, rapport d'enquête, p. 37 à 38.

utilisateur avant de lui attribuer des droits. Or, il est difficilement justifiable que la défenderesse collecte ces données supplémentaires pour cette finalité.

73. Par ailleurs, comme le fait remarquer le plaignant, il convient de souligner que la défenderesse ne dispose, en principe, d'aucune autre photo de l'utilisateur. Dès lors, la collecte de la photo figurant sur la carte d'identité ne peut être considérée comme nécessaire au regard de la finalité d'identification et d'authentification. En effet, en l'absence de tout élément de comparaison pour procéder à l'identification, une telle collecte est inutile.
74. De surcroît, la DPO de la défenderesse a elle-même reconnu que le numéro de carte d'identité eID a été collecté sans être nécessaire, en raison d'une « erreur de paramétrage technique ». Cet élément tend à confirmer que le processus de collecte mis en place était, en réalité, paramétré par défaut pour la collecte de l'ensemble des données ID via itsme. Cela démontre également un manquement à l'article 25.2 du RGPD, qui impose au responsable du traitement de garantir que, par défaut, seules les données nécessaires soient traitées.
75. Enfin, la Chambre Contentieuse note que les mêmes données étaient collectées tant lors de l'inscription que lors de chaque connexion ultérieure de l'utilisateur, comme l'a confirmé la DPO de la défenderesse. Cette collecte répétée de données excédentaires à chaque authentification illustre la portée concrète du manquement au principe de minimisation et l'absence de mesures de protection des données par défaut.
76. La Chambre Contentieuse conclut que la défenderesse a violé les articles 5.1.c) et 25.2 du RGPD en collectant des données excédentaires à la finalité d'authentification et d'identification poursuivie dans le cadre du service TruliUs, et en ne mettant pas en œuvre les mesures techniques et organisationnelles nécessaires pour garantir que, par défaut, seules les données nécessaires soient traitées.

### **III. Sanctions et mesures correctrices**

77. Aux termes de l'article 100, § 1er, de la LCA, la Chambre Contentieuse a le pouvoir de :
  - 1° classer la plainte sans suite ;
  - 2° ordonner le non-lieu ;
  - 3° prononcer une suspension du prononcé ;
  - 4° proposer une transaction ;
  - 5° formuler des avertissements et des réprimandes ;
  - 6° ordonner de se conformer aux demandes de la personne concernée d'exercer ses droits;
  - 7° ordonner que l'intéressé soit informé du problème de sécurité ;
  - 8° ordonner le gel, la limitation ou l'interdiction temporaire ou définitive du traitement ;
  - 9° ordonner une mise en conformité du traitement ;

- 10° ordonner la rectification, la restriction ou l'effacement des données et la notification de celles-ci aux récipiendaires des données ;
- 11° ordonner le retrait de l'agrément des organismes de certification ;
- 12° donner des astreintes ;
- 13° donner des amendes administratives ;
- 14° ordonner la suspension des flux transfrontières de données vers un autre État ou un organisme international ;
- 15° transmettre le dossier au parquet du Procureur du Roi de Bruxelles, qui l'informe des suites données au dossier ;
- 16° décider au cas par cas de publier ses décisions sur le site internet de l'Autorité de protection des données.

78. La Chambre Contentieuse estime que, sur la base des faits et de l'analyse qui précèdent, il y a lieu de conclure que la défenderesse a violé les dispositions suivantes du RGPD :

- Violation de l'**article 5.2 du RGPD**, en ce que la défenderesse s'est qualifiée de sous-traitante pour l'activité de traitement d'authentification et d'identification effectuée dans le cadre du service TruliUs, alors qu'elle devait être qualifiée de responsable du traitement et était dès lors tenue, à ce titre, de respecter l'ensemble des principes énoncés à l'article 5.1 du RGPD et d'être en mesure de démontrer cette conformité ;
- Violation des **articles 5.1.a), 12.1 et 13 du RGPD**, en raison de l'absence d'information complète, transparente et aisément accessible fournie au plaignant sur le traitement de ses données à caractère personnel dans le cadre du service TruliUs ;
- Violation des articles **5.1.a), 12.1 et 15.1 du RGPD**, en raison de l'absence de réponse de la défenderesse aux demandes d'accès que le plaignant lui a adressées les 11 et 19 mars 2021;
- Violation des articles **5.1.c) et 25.2 du RGPD**, en raison de la collecte excédentaire de données dans le cadre du service TruliUs et de l'absence de mesures techniques et organisationnelles garantissant que, par défaut, seules les données nécessaires soient traitées.

ci-après conjointement appelées les « **violations constatées** ».

79. L'ensemble des violations constatées s'inscrit dans une seule et même activité de traitement : celle d'authentification et d'identification mise en œuvre dans le cadre du service TruliUs. La qualification erronée de la défenderesse en tant que sous-traitante (article 5.2 du RGPD) est à l'origine des autres manquements. C'est en effet pour avoir refusé de se reconnaître responsable du traitement que la défenderesse n'a pas assumé les obligations de transparence (articles 5.1.a), 12.1 et 13), de facilitation de l'exercice des droits (articles 5.1.a), 12.1 et 15.1) et de minimisation des données (articles 5.1.c) et 25.2) qui lui

incombaient à ce titre. Ces manquements procèdent ainsi d'une volonté unitaire et sont étroitement liés.

80. Au regard de cette articulation, la Chambre Contentieuse estime qu'il y a lieu d'infliger une **amende administrative** pour la seule violation de l'article 5.2 du RGPD, qui constitue la violation prépondérante dont découlent l'ensemble des autres manquements constatés, et d'assortir cette amende d'une **réprimande** pour les autres violations constatées, en exécution de l'article 100, § 1er, 5° de la LCA.
81. Au regard des circonstances propres à la présente affaire, cette articulation se justifie à plusieurs titres. En premier lieu, sanctionner par une amende unique la violation à l'origine de l'ensemble des manquements permet de refléter le caractère structurel et indissociable de la situation litigieuse. En deuxième lieu, la réprimande, qui n'a pas de portée pécuniaire, garantit que les violations consécutives soient formellement constatées dans le dispositif de la décision et puissent ainsi exercer leur fonction pédagogique et dissuasive, tant à l'égard de la défenderesse qu'à l'égard de l'ensemble des acteurs du secteur. En troisième lieu, cette articulation préserve le caractère proportionné de la sanction globale, en évitant un alourdissement pécuniaire qui ne se justifierait pas dès lors que les violations consécutives sont la conséquence directe et exclusive de la qualification erronée déjà sanctionnée par l'amende. Le RGPD prévoit du reste expressément cette articulation : l'article 58.2.i) dispose que l'autorité de contrôle peut imposer une amende « en complément ou à la place » des autres mesures correctrices, et le considérant 148 confirme que « *des sanctions y compris des amendes administratives devraient être infligées [...] en complément ou à la place des mesures appropriées imposées par l'autorité de contrôle* ».
82. Dans le présent dossier, la Chambre Contentieuse décide donc d'adopter les mesures suivantes pour sanctionner les diverses violations du RGPD qu'elle a constatées :
- En exécution de l'article 58.2.i) du RGPD et des articles 100 §1er, 13° et 101 de la LCA, imposer à la défenderesse une amende administrative de **120.000 EUR** pour la violation de l'article **5.2 du RGPD** ;
  - En exécution de l'article 100, § 1er, 5° de la LCA, formuler, à l'égard de la défenderesse une réprimande pour la violation des articles **5.1.a), 5.1.c), 12.1, 13, 15.1 et 25.2 du RGPD**.
83. Selon le RGPD et les lignes directrices 04/2022 de l'EDPB sur le calcul des amendes<sup>52</sup> (ci-après les « **Lignes Directrices 04/2022** »)<sup>53</sup>, une autorité de contrôle comme l'APD a le pouvoir discrétionnaire de déterminer les mesures correctrices et les sanctions

<sup>52</sup> EDPB, Lignes directrices 04/2022 sur le calcul des amendes administratives au titre du RGPD, 24 mai 2023, disponible sur [https://www.edpb.europa.eu/system/files/2024-01/edpb\\_guidelines\\_042022\\_calculationofadministrativefines\\_fr\\_0.pdf](https://www.edpb.europa.eu/system/files/2024-01/edpb_guidelines_042022_calculationofadministrativefines_fr_0.pdf).

<sup>53</sup> EDPB, Lignes Directrices 04/2022, paragraphes 15, 20, 69, 84, 144.; RGPD, considérants 148, 150 ; art. 58.1.i), 83.

appropriées, et notamment le pouvoir discrétionnaire d'imposer une amende. Cette compétence découle spécifiquement des articles 51, 58 et 83 du RGPD, comme l'a confirmé la jurisprudence de la Cour des Marchés dans ses arrêts du 19 février 2020, 7 juillet 2021, ou encore du 20 décembre 2023<sup>54</sup>, qui ont mis en lumière l'étendue du pouvoir discrétionnaire de la Chambre Contentieuse concernant le choix des sanctions et l'ampleur de l'amende. La Chambre Contentieuse rappelle qu'en vertu du considérant 148 du RGPD, une amende administrative peut être imposée pour toute violation du règlement, y compris donc lors la première constatation d'une violation<sup>55</sup>.

84. Afin d'infliger dans chaque cas une amende effective, proportionnée et dissuasive, les autorités de contrôle doivent adapter les amendes administratives au cas d'espèce et peuvent se baser pour ce faire sur la méthode conçue par le l'EDPB à cet effet, reprise dans les Lignes Directrices 04/2022. L'application de la méthodologie reprise dans les Lignes Directrices 04/2022 a été suivie par la Chambre Contentieuse, car elle est recommandée pour garantir la cohérence de l'application du RGPD au sein de l'Union Européenne.
85. L'article 83 du RGPD établit les facteurs dont il faut tenir compte dans chaque cas concret pour décider si une amende administrative est infligée et, le cas échéant, pour en fixer le montant. Pour ce faire, la Chambre Contentieuse tient compte, dans cette appréciation, de la gravité des violations, de leur durée et de l'effet dissuasif nécessaire pour prévenir de futures violations, étant précisé que ces facteurs sont conjointement examinés dans l'évaluation détaillée ci-après, qui porte tant sur l'imposition de l'amende que sur son montant.

### **III.1. Montant de départ pour le calcul**

86. Comme indiqué plus haut, la Chambre Contentieuse a décidé de suivre la méthodologie pour le calcul des amendes prévue dans les Lignes directrices 04/2022<sup>56</sup>. Dans cette seconde étape, il est tenu compte de la classification des violations en fonction de leur nature en vertu de l'article 83, paragraphes 4 à 6, du RGPD, de la gravité de la violation et du chiffre d'affaires

---

<sup>54</sup> Cour des marchés, 19ème Chambre A, arrêt du 7 juillet 2021, 2021/AR/320 (accessible [ici](#)), p. 37-47 ; Cour des marchés, 19ème Chambre A, arrêt du 19 février 2020, 2020/AR/1160, (accessible [ici](#)) p. 30-31 ; Cour des marchés, 19ème Chambre A, arrêt du 20 décembre 2023, 2023/AR/817, (accessible [ici](#)) p. 57, 61 et 62.

<sup>55</sup> Le considérant 148 du RGPD énonce que : « Afin de renforcer l'application des règles du présent règlement, des sanctions y compris des amendes administratives devraient être infligées pour toute violation du présent règlement, en complément ou à la place des mesures appropriées imposées par l'autorité de contrôle en vertu du présent règlement. En cas de violation mineure ou si l'amende susceptible d'être imposée constitue une charge disproportionnée pour une personne physique, un rappel à l'ordre peut être adressé plutôt qu'une amende. Il convient toutefois de tenir dûment compte de la nature, de la gravité et de la durée de la violation, du caractère intentionnel de la violation et des mesures prises pour atténuer le dommage subi, du degré de responsabilité ou de toute violation pertinente commise précédemment, de la manière dont l'autorité de contrôle a eu connaissance de la violation, du respect des mesures ordonnées à l'encontre du responsable du traitement ou du sous-traitant, de l'application d'un code de conduite, et de toute autre circonstance aggravante ou atténuante. L'application de sanctions y compris d'amendes administratives devrait faire l'objet de garanties procédurales appropriées conformément aux principes généraux du droit de l'Union et de la Charte, y compris le droit à une protection juridictionnelle effective et à une procédure régulière ».

<sup>56</sup> EDPB, Lignes directrices 04/2022, *op. cit.*, p. 19.

de l'entreprise. Par ailleurs, il n'est pas nécessaire d'appliquer le mécanisme de plafonnement prévu à l'article 83.3 du RGPD, dès lors que la présente décision n'impose qu'une seule amende administrative, à savoir celle prononcée pour la violation de l'article 5.2 du RGPD.

### III.1.1. Classification de la violation en fonction de sa nature, en vertu de l'article 83, paragraphes 4 à 6 inclus du RGPD

87. Le RGPD fait une distinction entre deux catégories de violations : les violations qui sont punissables en vertu de l'article 83.4 du RGPD, d'une part, et les violations qui sont punissables en vertu des articles 83.5 et 83.6 du RGPD, d'autre part :

- l'amende maximale pour la première catégorie de violations s'élève à EUR 10.000.000 ou 2 % du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu.
- la deuxième catégorie peut conduire à une amende de maximum EUR 20.000.000 ou 4 % du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu.

88. En l'espèce, la Chambre Contentieuse retient le montant suivant:

- Pour la violation de l'**art. 5.2 du RGPD** : en application de l'article 83.5 a) du RGPD, la Chambre Contentieuse peut imposer une amende administrative allant jusqu'à 20.000.000 EUR ou, dans les cas d'une entreprise, jusqu'à 4% de son chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu.

### III.1.2. Le degré de gravité de la violation

89. Conformément aux Lignes directrices 04/2022, l'autorité de contrôle examine les facteurs de l'article 83.2.a), b) et g) à la lumière des circonstances du cas d'espèce et détermine, sur la base de cet examen, le degré de gravité de la violation, qui peut être qualifié de « faible », « moyen » ou « élevé ».

#### **i. Article 83.2.a) du RGPD - La nature, la gravité et la durée de la violation :**

90. **Quant à la nature de la violation**

91. La Chambre Contentieuse fait remarquer que le principe de responsabilité (*accountability*) consacré à l'article 5.2 du RGPD impose au responsable du traitement de respecter l'ensemble des principes relatifs au traitement énoncés à l'article 5.1 du RGPD et d'être en mesure de démontrer qu'il les respecte. Ce principe est essentiel à l'effectivité du RGPD. C'est en se reconnaissant comme responsable du traitement et en assumant pleinement les

obligations qui en découlent qu'il garantit le respect des principes du RGPD ainsi que des droits des personnes concernées. En l'espèce, en se qualifiant de sous-traitante pour l'activité de traitement d'authentification et d'identification au cœur du service TruliUs, la défenderesse s'est soustraite à l'ensemble des obligations qui lui incombent en sa qualité de responsable du traitement.

92. **Quant à la gravité de la violation**

93. La qualification erronée n'est pas un manquement isolé ou ponctuel. En effet, elle revêt un **caractère structurel**, en ce qu'elle a déterminé l'ensemble du cadre de conformité du service TruliUs et a conduit la défenderesse à ne pas assumer les obligations de transparence, de facilitation de l'exercice des droits et de minimisation des données qui lui incombent. Les conséquences concrètes de la qualification erronée se sont matérialisées au travers des autres violations constatées. Pendant toute la durée d'exploitation du service, aucune entité n'assumait effectivement les obligations du responsable du traitement à l'égard des utilisateurs pour l'activité d'authentification et d'identification, ce qui a compromis l'effectivité des garanties que le RGPD entend assurer. Concrètement, les utilisateurs du service TruliUs, et en particulier le plaignant, se sont trouvés confrontés à un traitement dont la portée excédait ce qui leur avait été annoncé (violation des articles 5.1.a), 12.1 et 13 du RGPD), à l'absence de réponse à leurs demandes d'accès (violation des articles 5.1.a), 12.1 et 15.1 du RGPD), ainsi qu'à une collecte de données excédant ce qui était strictement nécessaire à la finalité d'authentification (violation des articles 5.1.c) et 25.2 du RGPD).
94. S'agissant du **dommage** subi par le plaignant, la Chambre Contentieuse note d'abord qu'aucun dommage matériel direct n'a été établi en l'espèce. Le préjudice retenu tient à l'atteinte portée à l'effectivité des droits du plaignant, lequel n'a jamais été en mesure d'identifier l'entité responsable du traitement de ses données dans le cadre du service TruliUs. La défenderesse se présentait comme sous-traitante. **Z**, le client supposé responsable (sa propre société), ne disposait ni des informations ni de la maîtrise technique du traitement. Ce qui a eu pour conséquence que le plaignant s'est retrouvé dans l'impossibilité d'exercer effectivement ses droits. Faute d'avoir reçu une information complète lors de la collecte, il a sollicité l'accès auprès de la défenderesse les 11 et 19 mars 2021, sans obtenir de réponse. Le 29 mars 2021, il a saisi l'APD d'une plainte, puis a dû entrer dans une procédure contentieuse pour faire valoir des droits que le RGPD lui garantit.
95. S'agissant toutefois du **nombre de personnes concernées**, la Chambre Contentieuse observe qu'il demeure relativement limité, dès lors que la plateforme comptable est le seul partenaire à avoir effectivement intégré le service TruliUs. Le nombre d'utilisateurs susceptibles d'avoir été affectés par la qualification erronée se restreint ainsi aux personnes physiques ayant utilisé TruliUs pour s'authentifier auprès de la plateforme comptable, soit,

selon les déclarations de la défenderesse, environ 500 utilisateurs. Le service TruliUs a été conçu et commercialisé par la défenderesse afin d'être intégré par une pluralité de partenaires économiques. Dès lors, si la portée effective du traitement est demeurée limitée en pratique, sa portée potentielle, telle qu'elle résulte de la conception même du service et de son modèle de commercialisation, se voulait plus large. Le nombre restreint de personnes concernées s'explique probablement par la faible adoption du service et par son retrait du marché par la défenderesse en 2023.

### **Quant à la durée de la violation**

96. La Chambre Contentieuse fait remarquer que la qualification erronée de la défenderesse en tant que sous-traitante a persisté durant l'ensemble de la période d'exploitation de TruliUs, à savoir d'octobre 2020 (mise sur le marché de TruliUs) à mars 2023 (retrait du service), soit une période d'environ deux ans et demi. Il ne s'agit donc pas d'une violation ponctuelle mais d'une violation qui s'est prolongée sur plusieurs années.

### **ii. Article 83.2.b) du RGPD - Le caractère intentionnel et négligent de la violation :**

97. Concernant le **caractère intentionnel ou négligent de la violation** (critère repris à l'article 83.2.b) du RGPD) : selon la Chambre Contentieuse, il n'y a pas d'intention — manifeste — dans le chef de la défenderesse d'enfreindre délibérément ses obligations en matière de responsabilité au titre de l'article 5.2 du RGPD, mais l'élément moral de l'infraction est cependant établi en vertu des critères issus de la jurisprudence de la CJUE<sup>57</sup>. La négligence requiert un élément de conscience, mais pas un élément de volonté. Cet élément de conscience est rempli lorsque le destinataire d'une disposition ne pouvait pas ignorer le caractère infractionnel de son comportement, qu'il ait ou non conscience de violer certaines dispositions du RGPD. Dès lors, le facteur décisif est de savoir si le destinataire d'une disposition était en mesure de savoir que son comportement était illégal, et non s'il en avait effectivement conscience. Il est attendu du responsable de traitement qu'il s'informe et se familiarise avec le droit et les obligations qui lui sont applicables, dans le cadre de son devoir de diligence. À cet égard, les notions de responsable du traitement et de sous-traitant sont définies à l'article 4, points 7) et 8) du RGPD et leur portée a été précisée tant par la jurisprudence constante de la CJUE<sup>58</sup> que par les Lignes directrices 07/2020 de l'EDPB sur

<sup>57</sup> Voir CJUE, arrêt C-807/21, Deutsche Wohnen, ECLI:EU:C:2023:950, points 75 à 78.

<sup>58</sup> Voy. notamment CJUE, 5 juin 2018, Wirtschaftsakademie Schleswig-Holstein, C-210/16 ; CJUE, 29 juillet 2019, Fashion ID, C-40/17 ; CJUE, 10 juillet 2018, Jehovan todistajat, C-25/17.

les notions de responsable du traitement et de sous-traitant<sup>59</sup>, adoptées au début de la période d'exploitation de TruliUs. Ces sources fournissent aux opérateurs économiques avertis un ensemble de références suffisamment précis pour leur permettre de procéder à une qualification correcte de leur rôle au regard de chaque activité de traitement qu'ils mettent en œuvre.

98. En l'espèce, la défenderesse soutient, dans le huitième moyen de ses conclusions, que sa position sur sa qualité de sous-traitante a été cohérente depuis le début, comme l'attesteraient sa déclaration de confidentialité, ses conditions générales, son AIPD et son registre des activités de traitement, et qu'une éventuelle erreur de qualification ne saurait être constitutive d'une faute. En réaction au formulaire de sanction, la défenderesse ajoute que les notions de responsable du traitement et de sous-traitant feraient l'objet d'une insécurité juridique telle qu'aucune négligence ne saurait lui être reprochée, et que le caractère novateur du service TruliUs imposait une analyse pour laquelle aucun précédent jurisprudentiel ou ligne directrice spécifique n'était disponible. La Chambre Contentieuse ne peut suivre cet argumentaire, pour les motifs qui suivent.
99. Tout d'abord, la défenderesse occupe une position singulière en Belgique. Acteur central du secteur FinTech, Isabel SA développe et commercialise des services d'authentification destinés à être utilisés par d'autres entreprises selon un modèle B2B. À ce titre, elle conditionne, par les services qu'elle conçoit, le respect du RGPD par d'autres acteurs économiques. Le principe de responsabilité consacré à l'article 5.2 du RGPD impose à tout responsable du traitement, indépendamment de sa taille et de ses moyens, de procéder à une analyse rigoureuse de sa qualité. Ce devoir de diligence s'en trouve renforcé, eu égard à la fonction protectrice attendue d'un tel acteur central. Il l'est également d'autant plus par le fait que l'entité dispose d'un DPO désigné et qu'elle a réalisé une AIPD pour le service TruliUs, témoignant ainsi de l'existence, en interne, des ressources et de l'expertise nécessaires à l'accomplissement de cette analyse.
100. Il appartenait dès lors à la défenderesse, au regard de la diligence attendue d'un acteur de son envergure, de vérifier le bien-fondé de sa qualification à l'aune des critères du RGPD, des Lignes directrices de l'EDPB et de la jurisprudence précitée de la CJUE. La nouveauté du service TruliUs, n'amointrit pas la responsabilité du responsable du traitement, comme le prétend la défenderesse. Elle appelle au contraire un devoir de diligence renforcé puisque c'est précisément en l'absence de cadre préétabli qu'il revient au concepteur du service de procéder avec prudence dans l'analyse juridique de son rôle, eu égard à la responsabilité particulière qui pèse sur lui dans la définition d'un cadre de conformité approprié. Au moment de la conception du service TruliUs, et tout au long de ses deux années et demie d'exploitation, la défenderesse ne pouvait ignorer les conséquences absurdes de cette

---

<sup>59</sup> EDPB, Lignes directrices 07/2020, *op. cit.*

qualification erronée. Elle se considérait d'ailleurs elle-même comme responsable du traitement pour d'autres traitements liés au service TruliUs. En retenant la qualification de sous-traitante pour la seule activité d'authentification et d'identification, elle a procédé à un fractionnement artificiel d'activités de traitement intrinsèquement liées au sein d'un même service. Elle ne pouvait donc ignorer que la qualification de sous-traitante ne saurait être retenue pour une activité de traitement pour laquelle elle déterminait à la fois les finalités et les moyens essentiels. La cohérence avec laquelle la défenderesse a documenté et maintenu sa position de sous-traitante ne saurait, du reste, la dispenser d'une application correcte du RGPD. La Chambre Contentieuse n'ignore pas la complexité que peut soulever, dans certaines configurations, l'application des notions de responsable du traitement et de sous-traitant. En l'espèce, toutefois, Isabel a retenu une interprétation dont les conséquences absurdes ne pouvaient échapper à un opérateur averti. Soutenir, comme la défenderesse le fait, que Z serait responsable du traitement reviendrait à imposer au plaignant, en sa qualité de gérant de cette société, de se fournir à lui-même les informations relatives aux données collectées par la défenderesse (voy. violation des articles 5.1.a), 12.1 et 13 du RGPD), d'expliquer à lui-même la nécessité de la collecte excédentaire (voy. violation des articles 5.1.c) et 25.2 du RGPD) et d'exercer son droit d'accès auprès de sa propre société (voy. violation des articles 5.1.a), 12.1 et 15.1 du RGPD). Une telle position, qui réduit à néant l'effectivité des droits de la personne concernée, ne pouvait raisonnablement être tenue pour la solution exacte par un acteur diligent, et encore moins par un opérateur averti tel que la défenderesse.

101. La Chambre Contentieuse souligne enfin qu'admettre qu'une erreur de qualification puisse exonérer le responsable du traitement de sa responsabilité reviendrait à vider le principe de responsabilité de l'article 5.2 du RGPD de toute substance et, plus largement, à compromettre l'effectivité du RGPD. Il suffirait en effet à un responsable du traitement de se qualifier de sous-traitant pour se soustraire à la fois aux obligations que le RGPD lui impose et aux sanctions qui en garantissent le respect. Or, une telle situation place la personne concernée dans une position défavorable, car elle se trouve dans l'impossibilité concrète de faire valoir les droits que le RGPD lui confère. C'est précisément ce qui s'est produit en l'espèce, la qualification erronée de la défenderesse ayant conduit à ce que le plaignant ne reçoive pas d'information complète sur le traitement de ses données et se voie collecter des données excédentaires à la finalité poursuivie. La défenderesse invoque d'ailleurs ce même argument de qualification erronée pour justifier l'absence de réponse aux demandes d'accès du plaignant.
102. Au regard de l'ensemble de ces éléments, la Chambre Contentieuse considère que **l'élément moral de l'infraction est établi sous la forme d'une négligence.**

**iii. Article 83.2.g) du RGPD – Les catégories de données à caractère personnel concernées par la violation :**

103. La violation du principe de responsabilité résultant de la qualification erronée de la défenderesse concerne l'ensemble des données collectées dans le cadre de l'activité de traitement d'authentification et d'identification du service TruliUs, à savoir le nom, le prénom, l'adresse, le numéro de registre national, la date et le lieu de naissance, le numéro de carte d'identité électronique, la photo de la carte d'identité électronique, la nationalité, le sexe, l'adresse électronique et le numéro de téléphone.
104. Bien que ces données ne relèvent pas de catégories particulières au sens de l'article 9 du RGPD, la Chambre Contentieuse relève que cet ensemble comprend des données à caractère personnel particulièrement complètes qui, prises dans leur ensemble, permettent d'identifier de manière univoque une personne physique et présentent, dès lors, un risque accru. Le numéro de registre national fait par ailleurs l'objet d'une protection spécifique en droit belge, en vertu de la loi du 8 août 1983 organisant un Registre national des personnes physiques, qui en encadre strictement le traitement au-delà même des exigences du RGPD, et prévoit notamment des sanctions pénales à l'encontre des personnes qui utiliseraient le numéro de registre national sans y être habilitées.

**iv. Classification de la gravité de la violation et fixation du montant de départ adéquat :**

105. À la lumière des éléments exposés ci-avant, la Chambre Contentieuse conclut que la violation constatée est de gravité **moyenne**. Plusieurs éléments justifient cette qualification : (i) la qualification erronée présente un caractère structurel et constitue la cause directe des autres violations constatées (articles 5.1.a), 5.1.c), 12.1, 13, 15.1 et 25.2 du RGPD) puisque pendant toute la durée d'exploitation du service TruliUs, aucune entité n'a effectivement assumé les obligations du responsable du traitement à l'égard des utilisateurs, ce qui a eu pour conséquence concrète une collecte de données excédant la finalité d'authentification poursuivie, un défaut d'information complète et transparente sur le traitement, ainsi qu'une absence de réponse aux demandes d'accès du plaignant ; (ii) la violation a perduré durant environ deux ans et demi ; et (iii) elle a été le fait d'un acteur d'envergure du secteur FinTech occupant une position centrale en Belgique. Pour cette catégorie de gravité, l'EDPB fixe un montant de départ compris entre **10 et 20 %** du montant maximum légal prévu à l'article 83.5 du RGPD<sup>60</sup>.
106. Cela étant, la Chambre Contentieuse considère qu'il convient de positionner le montant de départ au seuil inférieur de cette fourchette, et non en son milieu ou en son haut. Trois éléments, propres aux circonstances de l'espèce, justifient ce positionnement : (i) le nombre

---

<sup>60</sup> EDPB, Lignes directrices 04/2022, *op. cit.*, point 60.

limité de personnes concernées, restreint au cercle des utilisateurs ayant recouru à TruliUs pour s'authentifier auprès de la plateforme comptable, soit environ 500 utilisateurs ; (ii) l'absence d'intention manifeste d'enfreindre les obligations du RGPD, le constat retenu étant celui d'une négligence ; et (iii) le caractère limité du dommage matériel direct subi par les personnes concernées. Ces éléments justifient le positionnement du montant de départ au seuil inférieur de la fourchette applicable aux violations de gravité moyenne. Les autres éléments soulevés par la défenderesse en réaction au formulaire de sanction seront examinés au stade de l'appréciation des circonstances aggravantes et atténuantes (voir ci-après).

107. La Chambre Contentieuse fixe dès lors le montant de départ pour le calcul ultérieur à **10 % du montant maximal légal** qui est repris à l'article 83.5 du RGPD.

**III.2. Le chiffre d'affaires de l'entreprise en tant qu'élément pertinent à prendre en compte en vue de l'imposition d'une amende effective, dissuasive et proportionnée en vertu de l'article 83.1 du RGPD**

108. Conformément à l'article 83.1 du RGPD, la Chambre Contentieuse doit veiller à ce que les amendes administratives imposées soient effectives, proportionnées et dissuasives. Elle introduit ainsi, dans la détermination du montant de départ, une distinction selon l'importance de l'entreprise.

109. Les articles 83.4 à 83.6 du RGPD établissent que le chiffre d'affaires annuel mondial total de l'exercice précédent doit être utilisé pour le calcul de l'amende administrative. À cet égard, le terme "précédent" doit être interprété conformément à la jurisprudence de la Cour de justice en matière de droit de la concurrence, de sorte que l'événement pertinent pour le calcul de l'amende est la décision de l'autorité de contrôle relative à l'amende, et non le moment de l'infraction sanctionnée<sup>61</sup>.

110. Les comptes annuels ont été consultés le 29 mars 2026 sur le site web de la Banque Nationale de Belgique (« BNB »). En l'espèce, bien que l'année de référence soit 2025, le bilan n'étant pas encore disponible pour l'exercice 2025 (étant généralement déposé en juin/juillet de l'année qui suit l'exercice), le seul élément objectif et vérifiable à disposition de la Chambre Contentieuse est le chiffre d'affaires pour l'exercice 2024. En l'absence de données plus récentes, la Chambre Contentieuse retient ce chiffre d'affaires comme base pour son calcul. Dans le cas d'espèce, il apparaît que le chiffre d'affaires de l'entreprise est établi à 65.087.031 euros pour l'année 2024. Ce chiffre ressort des comptes annuels de Isabel SA tels que déposés auprès de la BNB le 23 mai 2025<sup>62</sup>. Compte tenu de ce que le chiffre d'affaires de la défenderesse est resté stable au cours des années précédentes, la

<sup>61</sup> EDPB, Lignes directrices 04/2022, *op. cit.*, point 131.

<sup>62</sup> <https://consult.cbso.nbb.be/consult-entreprise/0455530509>.

Chambre Contentieuse estime que le chiffre d'affaires de l'exercice 2024 peut être pris en considération. Elle note également que, compte tenu du chiffre d'affaires de ces dernières années qui est resté relativement stable et autour de 65.000.000 euros, la défenderesse reste de toute façon dans la même catégorie d'entreprises selon les classifications par chiffre d'affaires effectuées par l'EDPB (à savoir, entreprises avec un chiffre d'affaires compris entre 50 et 100 millions d'euros<sup>63</sup>). Il convient enfin de relever que la défenderesse n'a pas contesté ces éléments dans sa réaction au formulaire de sanction.

111. Sur la base de ce qui précède, la Chambre Contentieuse constate que 4 % du chiffre d'affaires au cours de l'exercice précédent représentent 2.603.481,24 euros, ce qui est inférieur à 20.000.000 d'euros. **L'amende administrative maximale s'élève donc à 20.000.000 d'euros, conformément à l'article 83.5 du RGPD.** Concrètement, cela conduit au montant de départ suivant :

- Pour la violation de **l'article 5.2 du RGPD**, la Chambre Contentieuse a fixé le montant de départ pour le calcul ultérieur à **10%** du montant maximal légal qui est repris à l'article 83.5 du RGPD. **Cela conduit, en l'espèce, à un montant de départ de 2.000.000 d'euros.**

112. Conformément aux Lignes directrices de l'EDPB<sup>64</sup>, la Chambre Contentieuse peut, pour les entreprises dont le chiffre d'affaires annuel est compris entre 50 et 100 millions d'euros, envisager de procéder aux calculs sur la base d'une somme comprise entre 8 % et 20 % du montant de départ fixé. La Chambre Contentieuse conclut qu'en l'espèce, il est approprié de retenir un coefficient de **10 %** du montant de départ, se situant dans le bas de la fourchette applicable aux entreprises dont le chiffre d'affaires annuel est compris entre 50 et 100 millions d'euros. Ce coefficient prend en compte la situation financière de la défenderesse, sans pour autant méconnaître son statut d'acteur d'envergure dans le secteur FinTech belge. Cela conduit aux montants adaptés suivants :

113. Pour la violation de **l'article 5.2 du RGPD**, le montant de départ de 2.000.000 euros est **abaissé à 200.000 euros** (10 % du montant de départ).

114. Dans ce cadre, la Chambre Contentieuse tient compte du chiffre d'affaires de la défenderesse.

### **III.3. Circonstances aggravantes et atténuantes**

115. Selon le RGPD, après avoir évalué la nature, la gravité et la durée de la violation, le fait que la violation a été commise délibérément ou par négligence et les catégories de données à caractère personnel concernées par la violation (voir ci-dessus), l'autorité de contrôle doit

---

<sup>63</sup> EDPB, Lignes directrices 04/2022, *op. cit.*, point 66.

<sup>64</sup> EDPB, Lignes directrices 04/2022, *op. cit.*, point 66.

tenir compte des autres facteurs aggravants ou atténuants tels que repris à l'article 83.2 du RGPD<sup>65</sup>.

- a. Article 83.2.c) du RGPD – Toute mesure prise par le responsable du traitement ou le sous-traitant pour atténuer le dommage subi par les personnes concernées :** La défenderesse a retiré le service TruliUs du marché en mars 2023 et a procédé à la suppression des données traitées dans ce cadre, y compris les sauvegardes, à l'exception de certaines données du plaignant conservées afin de lui permettre de faire valoir ses droits dans le cadre de la présente procédure. Bien que ces mesures soient postérieures aux violations constatées et ne les effacent pas, elles ont eu pour effet de mettre fin au traitement litigieux et de prévenir tout dommage futur. Ce facteur est retenu au titre de **circonstance atténuante**.
- b. Article 83.2.d) du RGPD - Le degré de responsabilité du responsable du traitement ou du sous-traitant, compte tenu des mesures techniques et organisationnelles qu'ils ont mises en œuvre en vertu des articles 25 et 32 :** La défenderesse a désigné un DPO, réalisé une AIPD pour le service TruliUs, tenu un registre des activités de traitement et rédigé des conditions générales et une déclaration de confidentialité. Ces instruments de conformité, qui font partie des obligations incombant au responsable du traitement en vertu du RGPD, ont été mis en œuvre de manière documentée et cohérente, fût-ce sous la qualification erronée de sous-traitante. La Chambre Contentieuse relève que la qualification erronée en tant que sous-traitante a compromis l'efficacité de l'ensemble de ces mesures, dès lors que les obligations de transparence, de réponse aux demandes d'accès et de minimisation des données n'ont pas été effectivement assumées pour le traitement au cœur du service TruliUs. Toutefois, la cohérence avec laquelle la défenderesse a documenté et maintenu sa position au travers de ces instruments atteste d'une démarche de conformité réelle, qui se distingue d'une situation dans laquelle le responsable du traitement n'aurait mis en œuvre aucune mesure technique ou organisationnelle. Ce facteur est dès lors retenu au titre de circonstance **atténuante modérée**.
- c. Article 83.2.e) du RGPD - Toute violation pertinente commise précédemment par le responsable du traitement ou le sous-traitant :** La Chambre Contentieuse n'a pas connaissance de violation pertinente commise précédemment par la défenderesse au sens de cet article. Ce facteur est considéré comme **neutre**.

---

<sup>65</sup> EDPB, Lignes directrices 04/2022, *op. cit.*, point 70.

- d. Article 83.2.f) du RGPD - Le degré de coopération établi avec l'autorité de contrôle en vue de remédier à la violation et d'en atténuer les éventuels effets négatifs :** En l'espèce, la défenderesse a répondu aux demandes du Service d'Inspection et lui a communiqué les documents sollicités au cours de l'enquête. Pour autant, la Chambre Contentieuse rappelle que la coopération avec l'autorité de contrôle est une obligation légale, posée notamment par l'article 31 du RGPD et par l'article 65 de la LCA. Le simple fait de s'y soumettre ne suffit donc pas pour reconnaître une circonstance atténuante. Pour qu'une coopération soit retenue comme atténuante, comme l'indiquent les Lignes directrices 04/2022 de l'EDPB<sup>66</sup>, elle doit aller au-delà de ce qui est légalement requis et avoir effectivement contribué, par des initiatives propres au responsable du traitement, à atténuer les effets négatifs de la violation. Aucun élément du dossier n'établit une telle initiative. Quant aux mesures correctrices qui ont effectivement contribué à atténuer la violation (le retrait du service TruliUs et la suppression des données qui s'en sont suivies), elles ont déjà été prises en compte au titre de l'article 83.2.c) du RGPD. Ce facteur est par conséquent considéré comme **neutre**.
- e. Article 83.2.h) du RGPD - La manière dont l'autorité de contrôle a eu connaissance de la violation, notamment si, et dans quelle mesure, le responsable du traitement ou le sous-traitant a notifié la violation :** La Chambre Contentieuse a eu connaissance des violations par le biais de la plainte déposée par le plaignant le 29 mars 2021, et non par une notification spontanée de la défenderesse. Ce facteur est considéré comme **neutre**.
- f. Article 83.2.i) du RGPD - Lorsque des mesures visées à l'article 58, paragraphe 2, ont été précédemment ordonnées à l'encontre du responsable du traitement ou du sous-traitant concerné pour le même objet, le respect de ces mesures :** Aucune mesure visée à l'article 58.2 n'a été précédemment ordonnée à l'encontre de la défenderesse pour le même objet. Ce facteur est **sans objet**.
- g. Article 83.2.j) du RGPD - L'application de codes de conduite approuvés en application de l'article 40 ou de mécanismes de certification approuvés en application de l'article 42 :** La Chambre Contentieuse n'a pas d'information sur l'existence d'un code de conduite ni de mécanisme de certification. Ce facteur est **sans objet**.

---

<sup>66</sup> EDPB, Lignes directrices 04/2022, *op. cit.*, points 95 à 97.

**h. Article 83.2.k) du RGPD - Toute autre circonstance aggravante ou atténuante applicable aux circonstances de l'espèce, telle que les avantages financiers obtenus ou les pertes évitées, directement ou indirectement, du fait de la violation:** . La Chambre Contentieuse n'a pas connaissance d'autres circonstances aggravantes ou atténuantes pertinentes à ce titre. Ce facteur est considéré comme **sans objet**.

116. La Chambre Contentieuse tient compte, au titre des circonstances atténuantes : (i) du retrait du service TruliUs en mars 2023 et de la suppression des données traitées dans ce cadre (article 83.2.c du RGPD), qui ont effectivement mis fin à la situation litigieuse et prévenu tout dommage futur ; et (ii) de la cohérence avec laquelle la défenderesse a documenté et maintenu sa position au travers d'instruments de conformité, attestant d'une démarche de conformité réelle qui se distingue d'une situation dans laquelle aucune mesure n'aurait été mise en œuvre (article 83.2.d du RGPD). Ces deux facteurs, considérés dans leur ensemble, justifient une réduction substantielle du montant. À cet égard, la Chambre Contentieuse a, à la lumière de la réaction de la défenderesse et pour les motifs exposés ci-avant — tenant notamment à une appréciation plus restrictive des circonstances atténuantes —, réévalué à la baisse le montant initialement envisagé. La procédure de formulaire de sanction a, ce faisant, pleinement joué son rôle contradictoire. **La Chambre Contentieuse décide de diminuer le montant total de l'amende de 40 %, le faisant passer de 200.000 euros à 120.000 euros.**

#### III.4. Harmonisation avec les montants maximaux

117. Le montant maximal de l'amende dans le cas présent a déjà été calculé ci-dessus. Conformément à l'article 83.5.a) du RGPD, ce montant peut s'élever jusqu'à 20.000.000 d'euros ou jusqu'à 4 % du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu.

118. Le chiffre d'affaires annuel de la défenderesse **s'élève à 65.087.031 euros**. La Chambre Contentieuse constate que 4 % du chiffre d'affaires au cours de l'exercice précédent représentent 2.603.481,24 euros, ce qui est inférieur à 20.000.000 d'euros. **L'amende administrative maximale s'élève donc à 20.000.000 d'euros, conformément à l'article 83.5 du RGPD.**

119. Le montant total de l'amende s'élève en l'espèce à **120.000 euros**, ce qui est largement inférieur au montant maximal de **20.000.000 d'euros**. Les montants maximaux légaux sont donc respectés.

### III.5. Effet effectif, proportionné et dissuasif

#### **i. Effectivité**

120. Le considérant 148 du RGPD souligne que les amendes administratives doivent être infligées "*[a]fin de renforcer l'application des règles du présent règlement*". L'amende infligée doit dès lors être suffisamment élevée pour réaliser cette finalité.
121. La Chambre Contentieuse considère que l'amende totale de **120.000 euros** est appropriée pour renforcer l'application des principes fondamentaux ayant fait l'objet d'une violation, à savoir le principe de responsabilité (art. 5.2 du RGPD). L'amende vise à garantir que la défenderesse et, plus largement, les acteurs du secteur FinTech prennent la pleine mesure de l'importance d'une qualification correcte de leur rôle au regard des traitements qu'ils mettent en œuvre.

#### **ii. Proportionnalité**

122. Le principe de proportionnalité implique que les montants des amendes ne peuvent pas être disproportionnés au regard des finalités poursuivies et que l'amende infligée doit être proportionnée à la violation, considérée dans son ensemble, en tenant compte notamment de sa gravité.
123. En l'espèce, la violation a été jugée comme étant de gravité moyenne. Conformément au paragraphe 60 des Lignes directrices de l'EDPB, la Chambre Contentieuse **a fixé le montant de départ à 10 % du montant maximal légal applicable**, ce qui se situe dans le plus bas de la fourchette correspondante (entre 10 et 20 %). La Chambre Contentieuse a tenu compte, dans la fixation de ce pourcentage, du nombre limité de personnes concernées (environ 500 utilisateurs) et du caractère négligent, et non intentionnel, de la violation.
124. Par ailleurs, la Chambre Contentieuse tient également compte du chiffre d'affaires de la défenderesse, raison pour laquelle elle n'a utilisé **que 10 % du montant de départ** pour le calcul de l'amende, conformément au paragraphe 66 des Lignes directrices de l'EDPB pour les entreprises dont le chiffre d'affaires annuel est compris entre 50 et 100 millions d'euros.
125. En outre, la Chambre Contentieuse a décidé de réduire l'amende de **40 %** en raison des circonstances **atténuantes** identifiées, à savoir le retrait du service TruliUs du marché et la suppression des données, la cohérence avec laquelle la défenderesse a documenté et maintenu sa position au travers d'instruments de conformité
126. Le montant total de l'amende de **120.000 euros** représente environ **0,18 % du chiffre d'affaires de la défenderesse** et 0,6 % du montant maximal légal de 20.000.000 d'euros. Si la défenderesse estime que la présente amende mettrait irrémédiablement en danger sa viabilité économique, la Chambre Contentieuse l'invite à fournir les éléments pour le démontrer, conformément au paragraphe 140 des Lignes directrices 04/2022 de l'EDPB.

127. La défenderesse soutient en outre, en réaction au formulaire de sanction, que le montant envisagé serait disproportionné au regard de plusieurs décisions précédemment rendues par la Chambre Contentieuse, et notamment des affaires Black Tiger (décision 07/2024), Aéroport de Charleroi (décision 47/2022) et Roularta Media Group. La Chambre Contentieuse rappelle à cet égard que la méthode de calcul prévue par les Lignes directrices 04/2022 de l'EDPB, dont l'application est nécessaire à la cohérence du système de sanctions au sein de l'Union européenne, repose sur une appréciation circonstanciée propre à chaque espèce, intégrant la nature, la gravité et la durée de la violation, le degré de négligence, le chiffre d'affaires de l'entité concernée ainsi que les circonstances aggravantes et atténuantes. Les affaires invoquées par la défenderesse présentent des configurations factuelles, des chiffres d'affaires et des qualifications juridiques distinctes de celles de la présente affaire, de sorte qu'une comparaison brute des montants n'est pas pertinente. La Chambre Contentieuse rappelle que ses décisions antérieures ne constituent pas une jurisprudence à laquelle elle serait liée dans l'appréciation des affaires ultérieures, ce que la Cour des marchés a au demeurant souligné<sup>67</sup>. En sa qualité d'autorité administrative, la Chambre Contentieuse exerce dans chaque affaire un pouvoir d'appréciation autonome qui, pour l'imposition d'une amende administrative, s'inscrit dans le cadre méthodologique des Lignes directrices 04/2022 de l'EDPB et tient compte des circonstances propres à chaque espèce. Le principe de cohérence dans l'application du RGPD s'apprécie au regard de cette méthodologie commune et non par comparaison terme à terme avec les montants prononcés dans des affaires aux configurations différentes. Le montant final retenu en l'espèce, après réévaluation à la lumière des arguments soulevés en réaction au formulaire de sanction, se situe dans le plus bas possible de la fourchette prévue par les Lignes directrices pour une violation de gravité moyenne, après application d'une réduction substantielle de 40 % au titre des circonstances atténuantes.
128. La Chambre Contentieuse estime que l'amende est proportionnée.

### **iii. Effet dissuasif**

129. Lors de l'imposition d'une amende, la Chambre Contentieuse tient compte tant de la dissuasion spécifique que de la dissuasion générale. Une amende est dissuasive lorsqu'elle dissuade un particulier de violer les finalités et les réglementations reprises dans le droit de l'Union européenne.
130. Le caractère dissuasif de l'amende doit comporter deux dimensions. Dissuader la personne à laquelle l'amende est infligée de réitérer la violation à l'avenir mais également dissuader

---

<sup>67</sup> Cour des marchés, arrêt du 27 janvier 2021, 2020/AR/1333, p. 21.

d'autres personnes de répéter le comportement constitutif de la violation de la première personne.

131. Plusieurs facteurs établissent l'effet dissuasif d'une amende : la nature et le montant de l'amende et la probabilité que l'amende soit infligée sont déterminants à cet égard. Une amende doit être suffisamment élevée pour avoir un impact financier significatif sur l'entreprise qui commet la violation, tout en restant proportionnée à la gravité de la violation. En d'autres termes, le critère de la dissuasion recoupe celui de l'effectivité. Il importe que les entreprises ne puissent pas réaliser de bénéfices financiers sur la base d'un traitement illicite de données à caractère personnel.
132. Dans le cas présent, la Chambre Contentieuse considère que l'amende totale de **120.000 euros** est suffisamment dissuasive pour envoyer un signal clair tant à la défenderesse qu'à l'ensemble des acteurs du secteur FinTech. Cette amende représente environ **0,18%** du chiffre d'affaires de la défenderesse, ce qui constitue un impact financier perceptible sans mettre en péril la viabilité économique de l'entreprise. Elle vise à rappeler à cet acteur important du secteur financier et technologique, qui traite des données à caractère personnel particulièrement complètes dans le cadre de services d'authentification et d'identification, qu'il est tenu à une diligence particulière dans la mise en œuvre de ses obligations au titre du RGPD, et en particulier dans la qualification correcte de son rôle au regard des traitements qu'il met en œuvre.
133. Au-delà de la défenderesse elle-même, l'amende remplit une fonction de signal nécessaire à l'échelle du secteur, où les services d'authentification numérique se multiplient. Dans ce contexte, les questions de qualification de responsable du traitement et de sous-traitant se posent de manière récurrente aux opérateurs économiques qui conçoivent ce type de services. À défaut d'un montant suffisamment significatif, l'amende risquerait d'être perçue comme un coût marginal de fonctionnement et perdrait tout caractère dissuasif tant à l'égard de la défenderesse qu'à l'égard du secteur dans son ensemble. La Chambre Contentieuse souligne enfin, que la qualification erronée a permis à la défenderesse, pendant les deux années et demie d'exploitation du service, de ne pas supporter pleinement les coûts de mise en conformité afférents à un service qu'elle traitait à tort comme externe à ses obligations principales. Sans qu'il soit possible de chiffrer précisément cet avantage indirect, la Chambre Contentieuse ne saurait l'ignorer dans l'appréciation du caractère effectif et dissuasif de l'amende, dans la mesure où la sanction doit, à tout le moins, neutraliser l'avantage qui a pu résulter pour la défenderesse de cette économie de coûts de conformité.
134. La Chambre Contentieuse a également pris en considération l'argument de la défenderesse, soulevé en réaction au formulaire de sanction, selon lequel l'imposition d'une amende serait dépourvue d'effet utile, dès lors que la défenderesse aurait, depuis le retrait du service

TruliUs, pleinement aligné ses pratiques sur le RGPD. Toutefois, la sanction prévue à l'article 83 du RGPD ne poursuit pas exclusivement une finalité corrective, mais également une finalité dissuasive, à l'égard tant de la défenderesse, pour prévenir toute réitération à l'occasion de futurs services qu'elle serait amenée à développer, qu'à l'égard du secteur dans son ensemble. Le seul fait que la défenderesse ait, postérieurement à l'ouverture de la présente procédure, mis en conformité ses pratiques ne saurait priver l'amende de son utilité, sauf à vider cette sanction de toute portée pour les violations passées qui ne perdurent plus à la date de la décision. La cessation de la violation a, du reste, déjà été pleinement prise en compte au titre des circonstances atténuantes, à hauteur d'une réduction de 40 % du montant de départ.

135. La défenderesse soutient également, en réaction au formulaire de sanction, que la durée de la procédure (29 mars 2021 – date de la présente décision) serait constitutive d'une violation de l'article 6 § 1 de la Conv. EDH, lequel consacre le droit à un jugement dans un délai raisonnable. A cet égard, l'appréciation du caractère raisonnable du délai s'effectue *in concreto*, à la lumière des circonstances de la cause et au regard notamment de la complexité de l'affaire, du comportement du requérant, du comportement des autorités compétentes ainsi que de l'enjeu du litige pour l'intéressé<sup>68</sup>. En l'espèce, le délai écoulé s'explique par des éléments objectifs tenant à la complexité juridique du dossier et au respect des droits procéduraux de la défenderesse. Le traitement de cette plainte a nécessité une instruction approfondie par le Service d'Inspection (du 2 septembre 2021 au 11 septembre 2023), un échange complet de conclusions entre les parties, l'organisation d'une audition (15 décembre 2025) et une procédure de formulaire de sanction permettant à la défenderesse de faire valoir ses observations sur l'amende envisagée (notification du 13 avril 2026 et réaction du 4 mai 2026). Ces étapes constituent autant de garanties procédurales dont la défenderesse a bénéficié et dont la durée ne saurait, en elle-même, lui être présentée comme un préjudice. La défenderesse n'établit du reste aucun préjudice concret qui résulterait de la durée de la procédure dans l'exercice de ses droits de défense. Elle a pu présenter l'ensemble de ses moyens, a été entendue lors d'une audition contradictoire et a pu réagir au formulaire de sanction.
136. Au vu de l'évaluation susmentionnée ainsi que des circonstances propres à cette affaire, la Chambre Contentieuse estime donc qu'il est approprié, en vertu des articles 58.2.i) et 83 du RGPD et des articles 100, § 1<sup>er</sup>, 13<sup>o</sup> et 101 de la LCA, d'infliger à la défenderesse, pour ce qui concerne l'amende administrative:
- une amende administrative d'un montant de **120.000 EUR** en raison de la violation de l'article 5.2 du RGPD.

---

<sup>68</sup> Cour eur. D.H., 5 janvier 2010, *Impar Ltd c. Lituanie*, point 26.

#### **IV. Publication de la décision**

137. Compte tenu de l'importance de la transparence concernant le processus décisionnel de la Chambre Contentieuse, la présente décision est publiée sur le site Internet de l'Autorité de protection des données moyennant la suppression des données d'identification directes du plaignant et des personnes citées, qu'elles soient physiques ou morales, à l'exclusion de la défenderesse et de itsme (Belgian Mobile ID SA). La Chambre Contentieuse estime que la publication de la présente décision avec identification de la défenderesse poursuit plusieurs objectifs.
138. Elle vise tout d'abord un objectif d'intérêt général, compte tenu de l'importance des services fournis par Isabel pour l'écosystème financier belge et du fait qu'un grand nombre d'utilisateurs et d'acteurs économiques en Belgique recourent, directement ou indirectement, à ces services. La Chambre Contentieuse estime pertinent de donner à cette décision une publicité permettant de sensibiliser les personnes concernées aux droits qui sont les leurs en vertu du RGPD. À ce titre, même si la décision ne concerne de manière directe que le plaignant (dont les données d'identification ne sont pas publiées), elle présente également un intérêt pour une large partie du public.
139. L'identification de la défenderesse est par ailleurs nécessaire à la bonne compréhension de la décision et donc, à la matérialisation de l'objectif de transparence poursuivi par la politique de publication de ses décisions de la Chambre Contentieuse. Elle apparaît en outre inévitable, dès lors que les spécificités techniques et le caractère singulier du service TruliUs, tels que décrits dans la présente décision, permettent aisément d'en identifier l'opérateur. Autrement dit, même en l'absence de mention explicite du nom d'Isabel, les éléments factuels exposés qui sont nécessaires à la bonne compréhension de la décision, suffisent à réidentifier la défenderesse.
140. La Chambre Contentieuse a pris connaissance de la demande formulée par la défenderesse, en réaction au formulaire de sanction, tendant à la non-publication de la présente décision ou, à titre subsidiaire, à sa publication anonymisée. Toutefois, les motifs exposés ci-dessus, tirés tant de l'objectif d'intérêt général attaché à la transparence des décisions de la Chambre Contentieuse que du caractère identifiable de la défenderesse au regard des spécificités techniques du service TruliUs, justifient en l'espèce de divulguer les données d'identification directes de la défenderesse. La crainte exprimée par la défenderesse quant à l'atteinte que la publication porterait à sa réputation dans un secteur fortement régulé ne saurait prévaloir sur l'objectif de transparence et de sensibilisation du public, étant rappelé que la diligence en matière de protection des données constitue précisément l'un des éléments attendus des opérateurs économiques agissant dans un tel secteur.

141. Enfin, la Chambre Contentieuse tient à préciser que la présente décision mentionne la plateforme itsme (Belgian Mobile ID SA) en tant que fournisseur d'identité numérique sur lequel la défenderesse s'est appuyée pour assurer l'authentification des utilisateurs du service TruliUs. Ces mentions ont une finalité strictement descriptive du fonctionnement technique du service en cause et sont nécessaires à la bonne compréhension de l'activité de traitement objet de la présente décision. Belgian Mobile ID SA n'est pas partie à la présente procédure et n'est mise en cause à aucun titre par la présente décision et les violations constatées concernent exclusivement la défenderesse et le service TruliUs qu'elle a conçu.

**PAR CES MOTIFS,**

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

- En vertu **de l'article 58.2.i) du RGPD** et de **l'article 100 §1, 13° de la LCA**, lu conjointement avec l'article 101 de la LCA, imposer une amende administrative d'un montant de **120.000 EUR** à la défenderesse pour la violation de **l'article 5.2 du RGPD**.
- En vertu de **l'article 100, § 1er, 5° de la LCA**, d'adresser une réprimande à la défenderesse pour la violation des articles **5.1.a), 5.1.c), 12.1, 13, 15.1 et 25.2 du RGPD**.
- En vertu de **l'article 100, § 1er, 16° de la LCA**, de **publier** la présente décision sur le site internet de l'Autorité de protection des données.

Conformément à l'article 108, §1 de la LCA, un recours contre cette décision peut être introduit, dans un délai de trente jours à compter de sa notification, auprès de la Cour des Marchés (cour d'appel de Bruxelles), avec l'Autorité de protection des données comme partie défenderesse.

Un tel recours peut être introduit au moyen d'une requête interlocutoire qui doit contenir les informations énumérées à l'article 1034ter du Code judiciaire<sup>69</sup> (« **C. jud.** »). La requête interlocutoire doit être déposée au greffe de la Cour des Marchés conformément à l'article

<sup>69</sup> La requête contient à peine de nullité:

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

1034<sup>quinquies</sup> du C. jud.<sup>70</sup>, ou via le système d'information e-Deposit du Service Public Fédéral Justice (article 32<sup>ter</sup> du C. jud.).

(Sé). Hielke HIJMANS

Directeur de la Chambre Contentieuse

---

<sup>70</sup> La requête, accompagnée de son annexe, est envoyée, en autant d'exemplaires qu'il y a de parties en cause, par lettre recommandée au greffier de la juridiction ou déposée au greffe.