Chambre Contentieuse

Décision quant au fond 65/2025 du 3 avril 2025

Numéro de dossier : **DOS-2021-06312**

Objet : violation de la confidentialité de données à caractère personnel

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

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

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

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

Vu les pièces du dossier ;

A pris la décision suivante concernant :

Le défendeur : Le Service public fédéral Intérieur, ci-après le SPF Intérieur, dont le siège est établi à 1000 Bruxelles – rue de Louvain 1, inscrit à la BCE sous le numéro 0308.356.862, représenté par Me Bart Martel, Me Anneleen Van de Meulebroucke et Me Laura Deschuyteneer, ci-après "le défendeur".

I. Faits et procédure

1. Entre le 24 janvier 2020 et le 28 janvier 2020, des milliers de certificats eID (tant des certificats de signature que des certificats d'authentification) ont été enregistrés dans un système de journalisation de la transparence des certificats (*Certificate Transparency*) (CT-logs) de Google. Les certificats contenaient des données à caractère personnel, dont le numéro de Registre national (en tant que numéro de série de l'objet du certificat), le nom et le prénom du citoyen, le fait qu'il s'agit d'un ressortissant belge ou d'un étranger.

2. Le 22 octobre 2021, le Comité de direction de l'Autorité de protection des données (ci-après "APD") a décidé de saisir le Service d'Inspection de l'APD sur la base de l'article 63, 1° de la LCA[1], telle qu'elle était d'application au moment des faits ayant donné lieu à la présente procédure, étant donné que le Comité de direction estimait qu'il y avait des indices sérieux de l'existence d'une pratique susceptible de donner lieu à une infraction aux principes fondamentaux de la protection des données à caractère personnel.

3. Le 8 septembre 2022, l'enquête du Service d'Inspection est clôturée, le rapport est joint au dossier et celui-ci est transmis par l'inspecteur général au président de la Chambre Contentieuse (article 91, § 1er et § 2 de la LCA).

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

   1. violation de l'article 5.1, f) j° l'article 32 du RGPD étant donné qu'il y aurait absence d'une protection adéquate des données à caractère personnel ;
   2. violation de l'article 5.2 et de l'article 24.1 du RGPD étant donné que le défendeur n'assumerait pas pleinement sa responsabilité ;
   3. violation de l'article 25 du RGPD étant donné que le défendeur n'appliquerait pas une protection des données dès la conception ;
   4. violation des articles 33 et 34 du RGPD étant donné que le défendeur n'aurait pas notifié la fuite de données et n'aurait pas informé les citoyens touchés ; et
   5. violation de l'article 35 du RGPD étant donné que le défendeur a réalisé une analyse d'impact relative à la protection des données dans le cadre du traitement avec l'eID mais qu'il n'y aurait pas eu d'actualisation de l'analyse d'impact dans le cadre de la problématique du présent dossier, ni de planning d'actualisation à cet égard.

4. Le 30 septembre 2022, la Chambre Contentieuse décide, en vertu de l'article 95, § 1er, 1° et de l'article 98 de la LCA, que le dossier peut être traité sur le fond.

---

[1] Article 63, 1° de la LCA (de l'époque) : Art. 63. *Le service d'inspection peut être saisi : 1° lorsque le comité de direction constate qu'il existe des indices sérieux de l'existence d'une pratique susceptible de donner lieu à une violation des principes fondamentaux de la protection des données à caractère personnel, dans le cadre de la présente loi et des lois contenant des dispositions relatives à la protection du traitement des données à caractère personnel.*

5. Le 30 septembre 2022, le défendeur est informé par envoi recommandé des dispositions visées à l'article 95, § 2 ainsi qu'à l'article 98 de la LCA. Il est également informé, en vertu de l'article 99 de la LCA, des délais pour transmettre ses conclusions.

   La date limite pour la réception des conclusions en réponse du défendeur a été fixée au 11 novembre 2022.

6. Le 25 octobre 2022, le défendeur demande une copie du dossier (art. 95, § 2, 3° de la LCA), qui lui a été transmise le 25 octobre 2022.

7. Le 27 octobre 2022, le défendeur accepte également de recevoir toutes les communications relatives à l'affaire par voie électronique et manifeste son intention de recourir à la possibilité d'être entendu, ce conformément à l'article 98 de la LCA.

8. Le 3 novembre 2022, le défendeur demande un report en ce qui concerne la date limite du dépôt des conclusions. La nouvelle date limite pour la réception des conclusions en réponse du défendeur est fixée au 15 décembre 2022.

9. Le 7 novembre 2022, les parties sont informées du fait que l'audition aura lieu le 7 novembre 2022.

10. Le 15 décembre 2022, la Chambre Contentieuse reçoit les conclusions en réponse de la part du défendeur.

11. Le 20 janvier 2023, le défendeur demande le report de l'audition. Le 23 janvier 2023, le défendeur est informé du fait que l'audition aura lieu le 16 mars 2023.

12. Le 16 mars 2023, le défendeur est entendu par la Chambre Contentieuse. Lors de l'audition, la possibilité d'envisager une solution à l'amiable dans cette affaire est examinée, y compris l'instrument d'une proposition de transaction visé à l'article 100, § 1er, 4 de la LCA.

13. Le 22 mars 2023, le procès-verbal de l'audition est soumis aux parties.

14. Le 29 mars 2023, la Chambre Contentieuse reçoit du défendeur quelques remarques relatives au procès-verbal qu'elle décide de reprendre dans sa délibération.

15. Le 28 août 2023, le défendeur est informé du fait qu'une nouvelle audition aura lieu le 25 septembre 2023. Le défendeur est entendu le 25 septembre 2023.

16. Le 10 septembre 2024, la Chambre Contentieuse informe le défendeur de son intention de procéder à une transaction et transmet une proposition de transaction.

17. Le 21 mars 2025, la Chambre Contentieuse retire la proposition de transaction (étant donné qu'une transaction dans un délai relativement court semblait impossible) impliquant la poursuite de la procédure quant au fond.

II. Motivation

18. La loi du 19 juillet 1991 *relative aux registres de la population, aux cartes d'identité, aux cartes des étrangers et aux documents de séjour* régit notamment la carte d'identité électronique (ci-après : "eID").[2] L'eID comporte deux certificats : le certificat de signature et le certificat d'authentification qui comportent diverses données à caractère personnel du citoyen[3], dont notamment le numéro de Registre national.

19. Le défendeur est responsable du traitement pour l'émission des eID et y place également ces certificats conformément au Règlement européen (EU) 2019/1157 et au Règlement européen eIDAS.[4] Ces certificats d'authentification et de signature sont publics.

20. Chaque citoyen peut décider lui-même s'il souhaite activer les certificats et avec qui il les partage. Le citoyen partage ses certificats avec un tiers lorsqu'il doit s'identifier et le cas échéant s'authentifier (comme pour la connexion en ligne dans une application web ou lors de la lecture de l'eID) ou lorsqu'il signe un document par voie électronique et le transmet à une tierce partie. Ces certificats portent comme numéro de série le numéro de Registre national du citoyen. Les certificats de signature électronique et/ou d'authentification qui comportent le numéro de Registre national peuvent être conservés sans consentement préalable tant qu'ils sont nécessaires pour apporter la preuve de la signature électronique ou de l'authentification (article 8, § 3, quatrième alinéa de la loi du 8 août 1983 *organisant un registre national des personnes physiques*[5]).

21. Les certificats, que le citoyen peut utiliser librement pour s'identifier/s'authentifier ou apposer une signature électronique, comportent donc des données à caractère personnel de sorte que le RGPD s'applique aux traitements de ces données à caractère personnel. Les publier ailleurs ou les partager avec des tiers ou les traiter d'une autre façon n'est donc pas permis sans condition. La loi Registre national[6] interdit même l'utilisation du numéro de

---

[2] M.B., 3 septembre 1991.

[3] Les deux types de certificats sont conçus de manière à comporter les données (personnelles) suivantes du citoyen :

a. Un numéro de série identique au numéro de Registre national

b. Les prénoms

C. Le nom de famille

d. Le pays

e. La durée de validité (début/fin)

f. Le type d'usage i. *Non repudiation* (pour *Signature*) ii. *DigitalSignature* (pour *Authentication*)

g. La clé publique

[4] Voir en particulier l'annexe I du Règlement (UE) 2019/1157 du Parlement européen et du Conseil du 20 juin 2019 *relatif au renforcement de la sécurité des cartes d'identité des citoyens de l'Union et des documents de séjour délivrés aux citoyens de l'Union et aux membres de leur famille exerçant leur droit à la libre circulation*, JO L 188/67 du 12 juillet 2019 et l'article 6 du Règlement (UE) n° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 *sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE*, JO L 257173 du 28 août 2014 (ci-après le "Règlement eIDAS")

[5] M.B., 21 avril 1984.

[6] Loi du 8 août 1983 *organisant un registre national des personnes physiques*, M.B., 21 avril 1984.

Registre national sans autorisation et à d'autres fins que celles pour lesquelles ladite autorisation a été octroyée (article 8, § 8, deuxième alinéa de la loi Registre national). Des sanctions pénales sont prévues à cet égard (article 13, deuxième alinéa de la loi Registre national).

22. Le traitement litigieux dans la présente affaire consiste en la publication illicite d'environ 40.000 certificats de signature et d'authentification de citoyens belges dans un des CT-logs de Google, violant ainsi la confidentialité des données à caractère personnel. La question se pose de savoir qui doit être désigné comme responsable du traitement pour ce traitement litigieux.

23. Conformément à l'article 4.7 du RGPD, il y a lieu de considérer comme responsable du traitement : *"la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement."* Le responsable du traitement doit donc avoir un pouvoir décisionnel et avoir une influence sur le traitement de données à caractère personnel en question.[7]

24. Le Service d'Inspection indique dans son rapport que le défendeur doit être qualifié de responsable du traitement pour le traitement litigieux. Le Service d'Inspection fait valoir les arguments suivants à cet égard. Tout d'abord, le défendeur est responsable de veiller à l'identité du citoyen : le défendeur produit et distribue notamment les eID conformément à ce qui est mentionné sur le site Internet du défendeur. Ensuite, le Service d'Inspection souligne que le défendeur, après concertation avec le SPF Stratégie et Appui (SPF BOSA)[8], a répondu aux questions lors de l'enquête d'inspection. Le Service d'Inspection fait remarquer qu'il ressort également des informations de la Banque-Carrefour des Entreprises (BCE) que le défendeur doit être considéré comme responsable du traitement. Il en joint un extrait au rapport.

25. Le défendeur conteste cette qualification en tant que responsable du traitement et réfute les constatations du Service d'Inspection. Il reconnaît être en effet compétent pour l'émission notamment des cartes eID mais fait valoir que cela n'indique rien quant au traitement litigieux dans cette affaire, à savoir la publication des certificats sur les CT-logs. Le défendeur place les certificats sur les eID des citoyens, mais ensuite ni le défendeur, ni le SPF BOSA, ni leurs sous-traitants ne publient ces certificats à un quelconque autre endroit. En ce qui concerne le fait qu'il a répondu aux questions du Service d'Inspection, le défendeur souligne qu'il s'est concerté avec le SPF BOSA et que lors de cette concertation, il a été convenu qu'il répondrait aux questions posées. Selon le défendeur, le fait d'avoir répondu aux questions du Service d'Inspection ne peut pas permettre de déduire une qualification en

[7] EDPB, Lignes directrices 7/2020 concernant les notions de "responsable du traitement" et de "sous-traitant" dans le RGPD, Version 2.0, adoptées le 7 juillet 2021, point 12.

[8] Le SPF BOSA est responsable du *Belgium Root CA* avec lequel le *Citizen CA* et le *Foreigner CA* sont signés.

tant que responsable du traitement pour la publication des certificats sur les CT-logs. Qui plus est, il a souligné à plusieurs reprises dans ses échanges avec le Service d'Inspection qu'il n'était pas le responsable du traitement pour le traitement visé. En ce qui concerne la dernière constatation quant à l'extrait de la BCE, le défendeur ne comprend pas clairement ce que le Service d'Inspection vise par là. L'extrait tel que repris dans le rapport d'inspection ne comporte pas d'indices intrinsèques quant au traitement de données à caractère personnel dans quelque contexte que ce soit, ni quant à l'eID et plus spécifiquement encore quant à la publication des certificats sur les CT-logs, conclut le défendeur.

26. Il appartient à la Chambre Contentieuse d'évaluer si le défendeur doit être désigné comme responsable du traitement pour la publication litigieuse des certificats sur les CT-logs.

27. La Chambre Contentieuse souligne qu'un responsable du traitement est responsable de son propre traitement "qu'il effectue lui-même ou qui est réalisé pour son compte" (considérant 74 du RGPD). La Cour de justice a estimé sur ce point qu'un responsable du traitement ne peut pas être responsable de traitements antérieurs ou postérieurs dont il n'a pas défini les finalités et les moyens :

"*En revanche, et sans préjudice d'une éventuelle responsabilité civile prévue par le droit national à cet égard, cette personne physique ou morale ne saurait être considérée comme étant responsable, au sens de ladite disposition, des opérations antérieures ou postérieures de la chaîne de traitement dont elle ne détermine ni les finalités ni les moyens*".[9]

28. Les lignes directrices 07/2020 *concernant les notions de "responsable du traitement" et de "sous-traitant" dans le RGPD* du Comité européen de la protection des données (European Data Protection Board, EDPB) indiquent également que la qualification de responsable du traitement ou de sous-traitant doit être évaluée à l'égard de chaque activité de traitement spécifique. La qualification de responsable du traitement ne découle donc pas simplement de la nature de l'entité qui traite des données, mais de ses activités concrètes dans un contexte spécifique.[10] Le fait que le site Internet du défendeur mentionne qu'il veille à l'identité du citoyen et délivre notamment les eID ne signifie pas dès lors qu'il serait automatiquement responsable du traitement pour tous les traitements de données à caractère personnel qui ont lieu par l'intermédiaire de l'eID, comme lors de l'utilisation ultérieure de l'eID et des certificats qui y sont placés par un citoyen ou un tiers, par exemple lors de la publication de données à caractère personnel dans les CT-logs.

29. La Chambre Contentieuse ne dispose d'aucun élément indiquant que le défendeur aurait décidé de procéder à la publication des certificats dans les CT-logs, et donc pas non plus sur le pourquoi et le comment de cette publication. Le Service d'Inspection constate également

[9] CJUE, 29 juillet 2019, affaire C-40/17, ECLIEUC:2019.629, *Fashion ID*, par. 74.

[10] EDPB, Lignes directrices 7/2020 concernant les notions de "responsable du traitement" et de "sous-traitant" dans le RGPD, Version 2.0, adoptées le 7 juillet 2021, point 14.

dans son rapport que "le traitement par l'écosystème CT n'a en effet pas été défini comme finalité par [le défendeur]".

30. Après examen par le défendeur et d'autres acteurs concernés tels que Google, on ne sait pas clairement qui a publié les certificats dans les CT-logs. Étant donné que les CT-logs sont une plateforme open source et qu'ils visent à prévenir des certificats erronés ou frauduleux, chacun peut (et doit) (pouvoir) charger des certificats dans les CT-logs. Google ne tient pas une journalisation détaillée de qui publie quoi dans ses CT-logs. Dès lors, Google elle-même ne peut pas retrouver qui a publié les certificats sur les CT-logs.

31. Vu ces éléments, la Chambre Contentieuse conclut qu'il n'est pas établi que le défendeur a défini *de jure* ou *de facto* la finalité et les moyens de la publication litigieuse des certificats et que dans ce contexte, le défendeur ne peut donc pas être désigné comme responsable du traitement.

32. Dès lors, la Chambre Contentieuse ne retient pas les constatations du Service d'Inspection et décide de procéder à un classement sans suite technique, conformément à sa politique de classement sans suite.[11]

33. La Chambre Contentieuse souligne toutefois que ni la loi Registre national, ni le RGPD ne permettent la publication de ces certificats et des données à caractère personnel y afférentes sur les CT-logs sans base juridique applicable. Les données à caractère personnel en question sont notamment le numéro de Registre national (en tant que numéro de série du certificat), la clé unique à de nombreuses données à caractère personnel authentiques du citoyen. L'utilisation de ces certificats rend public le numéro de Registre national, comme dans le cas d'une signature électronique ou d'une authentification en ligne. Néanmoins, la fuite illicite de milliers de certificats vers les CT-logs implique une amplification extrême de cette faille en termes de protection des données. En outre, cet enregistrement ne peut pas être effacé du CT-log concerné de Google, mais le CT-log lui-même peut bel et bien être effacé. Cet effacement a fait l'objet d'un suivi et d'une constatation par le défendeur lui-même. La confidentialité des données à caractère personnel était toutefois déjà violée à grande échelle et il existe un risque plus que significatif qu'à l'avenir, le traitement illicite des certificats eID et des numéros de Registre national qui y sont repris puisse constituer un problème récurrent (aussi dans un autre contexte que les CT-logs).

34. La Chambre Contentieuse souligne la gravité importante des risques pour les droits et libertés des personnes vu l'ampleur, le type de données à caractère personnel comme le numéro de Registre national, le catalyseur (le système CT-log) et le caractère presque

[11] Voir également la Décision 117/2021 du 22 octobre 2021 et la Politique de classement sans suite de la Chambre Contentieuse du 18 juin 2021, rubrique 3.1.A, consultable via le lien suivant : https://www.autoriteprotectiondonnees.be/publications/politique-de-classement-sans-suite-de-la-chambre-contentieuse.pdf.

ineffaçable[12]. La Chambre Contentieuse indique qu'une fois que les certificats sont publiés dans les CT-logs, ces certificats tombent dans le domaine public de sorte que plus aucun contrôle n'est possible quant à leur utilisation ultérieure par des tiers.

35. La Chambre Contentieuse insiste dès lors pour que l'on prenne ses responsabilités au niveau de l'Autorité fédérale afin d'élaborer une solution, avec tous les acteurs concernés tels que le défendeur, le SPF BOSA et potentiellement d'autres parties. Il est important qu'à court terme, des initiatives soient prises afin de limiter les risques pour la protection des données à caractère personnel.

III. Publication de la décision

36. Vu l'importance de la transparence concernant le processus décisionnel de la Chambre Contentieuse, la présente décision est publiée sur le site Internet de l'Autorité de protection des données, avec communication directe des données d'identification du défendeur.

PAR CES MOTIFS,

la Chambre Contentieuse de l'Autorité de protection des données décide, après délibération, en vertu de l'article 100, § 1er, 1° de la LCA, de classer la présente plainte sans suite.

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

Ce recours peut être introduit au moyen d'une requête contradictoire qui doit reprendre les mentions énumérées à l'article 1034*ter* du Code judiciaire[13]. La requête contradictoire doit être

[12] Rapport d'inspection du Service d'Inspection, p.12.

[13] 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.

déposée au greffe de la Cour des marchés conformément à l'article 1034*quinquies* du Code judiciaire[14], ou via le système informatique e-Deposit de la Justice (article 32*ter* du Code judiciaire).

(sé.) Hielke Hijmans

Président de la Chambre Contentieuse

[14] 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.