Avis n° 100/2019 du 3 avril 2019

Objet : demande d'avis relatif à un projet d'arrêté royal *modifiant l'arrêté royal du 25 mars 2003 relatif aux cartes d'identité* (CO-A-2019-087)

L'Autorité de protection des données (ci-après l' "Autorité") ;

Vu la loi du 3 décembre 2017 *portant création de l'Autorité de protection des données*, en particulier les articles 23 et 26 (ci-après "la LCA") ;

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 30 juillet 2018 *relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel* (ci-après "la LTD") ;

Vu la demande d'avis de Monsieur Pieter De Crem, Ministre de la Sécurité et de l'Intérieur, reçue le 28/02/2019 ;

Vu les informations complémentaires reçues les 15/03/2019 et 20/03/2019 ;

Vu le rapport de Monsieur Willem Debeuckelaere ;

Émet, le 3 avril 2019, l'avis suivant :

I. OBJET DE LA DEMANDE

La loi du 25 novembre 2018 *portant des dispositions diverses concernant le Registre national et les registres de population* a notamment modifié les articles 6 et 6*ter* de 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*. À la suite de cette modification, les nouvelles cartes d'identité qui seront délivrées comporteront d'ici peu une image numérisée des empreintes digitales du titulaire de la carte qui sera lisible de manière électronique.

Il était prévu que le Roi détermine par arrêté délibéré en Conseil des ministres et après avis de l'Autorité de protection des données les conditions et modalités de capture de l'image numérisée des empreintes digitales. C'est à cette fin que l'arrêté royal du 25 mars 2003 *relatif aux cartes d'identité* (ci-après l'arrêté royal) est adapté par le projet d'arrêté royal soumis pour avis, ci-après le projet. On profite de l'occasion pour procéder à plusieurs autres adaptations.

Du point de vue du traitement de données, une attention particulière doit être accordée aux points suivants :

- la puce électronique utilisée et l'apposition d'un code-barres bidimensionnel ;
- l'exigence de la présentation d'un certificat médical daté de moins d'un mois afin d'apporter la preuve de l'impossibilité de signer en raison d'un handicap physique ou mental ou d'une maladie (normalement, le titulaire de la carte d'identité doit apposer sa signature sur le document de base) ;
- les dispositions visant à régler qui prélève les empreintes digitales et selon quelles modalités ;
- la définition des cas dans lesquels aucune empreinte digitale ne sera insérée sur la carte d'identité ;
- la non-délivrance d'une carte d'identité en cas de doute sur l'identité du titulaire ;
- la révision de la procédure de déclaration en cas de perte, vol ou destruction de la carte d'identité.

II. REMARQUE PRÉALABLE

Le SPF Intérieur, ci-après le demandeur, a transmis, à titre confidentiel, son AIPD à l'Autorité. Le volet technique de l'avis comprend une synthèse de l'analyse des risques sur la base des informations contenues dans cette AIPD. Le commentaire circonstancié de l'Autorité sur l'AIPD est joint en annexe du présent avis mais ne sera pas publié, vu le caractère confidentiel.

III. EXAMEN DU PROJET

A. Base juridique

1. La délivrance d'une carte d'identité ou d'une carte d'étranger va de pair avec le traitement de données à caractère personnel tel que prescrit par l'article 6 de la loi du 19 juillet 1991.

2. Tout traitement de données à caractère personnel doit reposer sur un fondement juridique au sens de l'article 6 du RGPD. Vu le cadre réglementaire de la carte d'identité et de la carte d'étranger, les traitements auxquels elles donnent lieu semblent pouvoir trouver une base juridique dans l'article 6.1.c) ou e) du RGPD[1]. Il appartient au demandeur de préciser cette base juridique.

3. Dans ce contexte, l'Autorité attire certes l'attention sur l'article 6.3 du RGPD qui - lu conjointement avec l'article 8 de la CEDH et l'article 22 de la Constitution - prescrit que la réglementation qui encadre le traitement de données à caractère personnel doit en principe mentionner au moins les éléments essentiels suivants de ce traitement :

- la désignation du responsable du traitement ;
- la finalité du traitement ;
- les types ou catégories de données à caractère personnel qui feront l'objet du traitement ;
- les personnes concernées ;
- les entités auxquelles les données à caractère personnel peuvent être communiquées et les finalités pour lesquelles elles peuvent l'être ;
- les durées de conservation.

4. On examinera ci-après dans quelle mesure ces éléments essentiels se retrouvent dans les dispositions légales pertinentes et dans les dispositions y afférentes du projet.

5. Remarque : les observations formulées ci-après concernant la carte d'identité s'appliquent également, par extension et par analogie, à la carte d'étranger.

B. Responsable du traitement

6. Dans le processus qui conduit à la délivrance d'une carte d'identité, il n'est pas précisé de manière univoque qui est (sont) le(s) responsable(s) du traitement :

[1] C'est bien entendu le responsable du traitement lui-même qui est le mieux placé pour déterminer quelle base juridique correspond aux traitements de données à caractère personnel qui sont envisagés.

- L'article 6, § 1er, premier alinéa de la loi du 19 juillet 1991 dispose que la commune délivre une carte d'identité ou une carte d'étranger en tant que certificat d'inscription dans les registres de la population.
- En vertu de l'article 6, § 5, premier alinéa, l'autorité fédérale met à la disposition de la commune le matériel technique nécessaire à la carte électronique.
- L'article 3 de l'arrêté royal spécifie que le Ministre de l'Intérieur fournit la carte d'identité aux administrations communales et établit le modèle du document de base de la carte d'identité.
- Dans les *Instructions générales relatives aux cartes d'identité électroniques de Belges*[2] du SPF Intérieur, on retrouve ce qui suit : "*Le Registre national des personnes physiques est la plaque tournante du système. Ce service assure la coordination entre le demandeur de la carte d'identité électronique dans la commune et le contact avec le producteur, le personnalisateur et l'initialisateur de la carte. Toutes les étapes du processus de production sont signalées au Registre national. Le RN demande également à l'autorité de certification les certificats d'identité et de signature électronique. L'initialisateur prépare les clés de sécurité. Le RN vérifie si la paire de clés attribuée est unique : la clé publique est contrôlée, la clé privée n'est pas connue. Le RN prépare les données pour demander un certificat pour la paire de clés contrôlée : le RN attribue le numéro du certificat et demande à une autorité de certification agréée de délivrer un certificat. L'agrément de l'autorité de certification satisfait aux conditions de la loi du 9 juillet 2001 fixant certaines règles relatives au cadre juridique pour les signatures électroniques et les services de certification et aux exigences européennes en la matière. Le Registre national des personnes physiques tient un fichier central des cartes d'identité appelé "Registre des cartes d'identité*".

7. Dans l'AIPD que l'Autorité a reçue, il est précisé en page 4 que le SPF Intérieur est le responsable du traitement, plusieurs sous-traitants sont identifiés et il est fait mention de partenaires. En matière de traitement de données, le RGPD ne reconnaît pas de partenaires. Il reconnaît uniquement des responsables du traitement, des responsables conjoints du traitement, des sous-traitants et des tiers (article 4.7), 8) et 10) et article 26 du RGPD).

8. La délivrance de cartes d'identité requiert un traitement massif de données qui s'accompagne de toute une série de processus de traitement et l'implication d'un large éventail d'acteurs (SPF Intérieur, communes, producteur, firmes ICT,…). Il est grand temps que la réglementation identifie qui est (sont) le(s) responsable(s) (conjoints)/sous-traitant de quoi, de manière à ce qu'il soit clair pour chacun de savoir sur qui repose la responsabilité de veiller à ce que tant les dispositions du

[2] https://www.ibz.rrn.fgov.be/fileadmin/user_upload/fr/cartes/eid/instructions/IG-eID-25052018.pdf (version coordonnée du 2 mai 2017, dernière mise à jour le 25 mai 2018).

RGPD que les dispositions légales spécifiques soient respectées en la matière. Selon le cas, il faudra respecter soit l'article 24, soit l'article 26 ou l'article 28 du RGPD.

C. Finalité du traitement

9. À la lecture de l'article 6 de la loi du 19 juillet 1991 et de l'article 3 de l'arrêté royal, sans que cela soit formulé textuellement, on peut déduire que la carte d'identité est fournie et dès lors, que des données à caractère personnel sont traitées à cet effet pour les finalités suivantes :

- apporter la preuve qu'une personne est inscrite dans les registres de la population (article 6, § 1er, premier alinéa de la loi du 19 juillet 1991) ;
- établir l'identité d'une personne (article 1er et article 3, § 1er, premier alinéa de l'arrêté royal) ;
- permettre d'identifier et d'authentifier une personne à distance de manière électronique.

10. Ces finalités doivent par ailleurs être déterminées, explicites et légitimes (article 5.1.b) du RGPD).

11. L'Autorité constate que le législateur a approuvé l'enregistrement des empreintes digitales car le ministre compétent a insisté sur la nécessité de renforcer la lutte contre la fraude à l'identité (ce qui peut être qualifié de finalité manifestement compatible avec celles mentionnées au point 9). Toutefois, l'AIPD transmise par le demandeur mentionne ce qui suit : "*La justification de la finalité concernant la vérification de l'identité peut être améliorée, la justification liée à la lutte contre la fraude à l'identité ne tient pas.*" Dans l'AIPD, on change donc d'avis. On y souligne à présent que la carte d'identité est un document de voyage et doit dès lors répondre aux exigences internationales d'un document de voyage, un argument qui a été évoqué indirectement lors de la discussion parlementaire.

12. La carte d'identité n'a pas été conçue en tant que document de voyage, comme cela ressort des finalités. Le fait que plusieurs pays acceptent la carte d'identité belge comme document de voyage est la conséquence d'un accord avec les pays pour lesquels la carte d'identité telle qu'elle existe actuellement constitue une alternative fiable suffisante au passeport et ne doit donc pas avoir toutes les caractéristiques d'un passeport.

13. D'ailleurs, un pourcentage non négligeable de Belges ne voyage pas. À leur égard, l'enregistrement des empreintes digitales sur la carte d'identité est donc une mesure manifestement disproportionnée à la lumière de l'article 5.1.c) du RGPD. Et pour les Belges qui voyagent : pourquoi ne pas leur laisser le choix entre une carte d'identité avec les empreintes digitales ou un passeport ?

14. La durée de validité de la carte d'identité est de 10 ans. D'après les informations complémentaires, les empreintes digitales ne seront intégrées que lors du renouvellement des cartes d'identité. Cela veut donc dire que pendant 10 ans, 2 sortes de cartes d'identité seront en circulation. On peut dès lors s'interroger sur l'utilité de l'opération qui prendra 10 ans et donc aussi sur l'utilité d'intégrer les empreintes digitales sur la carte d'identité. Cela semble indiquer une fois encore que la fraude à l'identité n'est pas un problème si important et si grave qu'on l'a laissé entendre. L'AIPD confirme d'ailleurs cette constatation.

D. Données et proportionnalité

15. Les données mentionnées sur la carte d'identité et donc collectées à cette fin sont définies par l'article 6 de la loi du 19 juillet 1991, définition qui a déjà fait l'objet d'avis de l'Autorité[3], auxquels il est fait référence ici dans un souci d'exhaustivité.

D.1. Puce électronique (remplace le microprocesseur électronique)

16. Pour un commentaire détaillé sur la puce électronique, il est renvoyé au rapport d'analyse technique en annexe.

17. L'article 6, § 4, deuxième alinéa de la loi du 19 juillet 1991 dispose que : "*Le numéro de Registre national et la photographie du titulaire ne peuvent être utilisés que si cette utilisation est autorisée par ou en vertu d'une loi, d'un décret ou d'une ordonnance. (...)*". Un beau principe qui ne vaut rien dans la pratique. La photographie, qui est aussi obligatoirement enregistrée sur la puce de manière numérisée, n'est protégée en aucune manière. L'autorité publique fournit donc au citoyen un instrument n'offrant pas une protection spécifique pour cette donnée. Le citoyen n'a aucun contrôle des données qui peuvent ou non être lues de manière électronique. L'Exposé des motifs réfute cette objection comme suit[4] :

> *"La Commission recommande également que la loi impose aux responsables de traitement concernés de mettre en place des outils permettant à la personne concernée de décider des données qu'elle communique au moyen de sa carte (cf. point 75). Cependant, cette possibilité n'est pas envisageable car trop complexe pour le citoyen."*

18. En attendant, le concept actuel de la carte d'identité électronique date d'il y a 15 ans. La question se pose de savoir si entre-temps, on a examiné sérieusement si, compte tenu de l'état

[3] L'avis n° 19/2018 du 28 février 2018 de la Commission de la protection de la vie privée et l'avis n° 106/2018 du 17 octobre 2018 de l'Autorité.

[4] Chambre, doc 54 - 3256/001 - p. 39.

actuel de la technologie, il est possible de délivrer au citoyen une carte lui permettant de mieux protéger ses données. Actuellement, la carte d'identité peut difficilement être considérée comme un exemple de privacy by design (protection de la vie privée dès la conception).

19. Le citoyen est démuni. Il est tout simplement obligé de se baser sur la bonne foi de chaque personne qui lit sa carte d'identité. Lorsqu'il consent à la lecture de sa carte, il n'a aucune garantie que les informations qui sont lues, dont la photographie, ne sont pas non plus enregistrées. Lorsque sa carte est volée ou qu'il la perd, le vol d'identité est toutefois très facile.

D.2. Code-barres bidimensionnel

20. Le projet - article 3, 1° - instaure toutefois une nouveauté réglementaire. Il est en effet précisé explicitement que la carte d'identité contiendra un code-barres bidimensionnel. Il ressort des informations complémentaires fournies par le demandeur le 15/03/2019 que l'article 6 de la loi du 19 juillet 1991 a donné lieu, dans la pratique, à l'utilisation de 2 systèmes de données à caractère personnel lisibles de manière électronique sur la carte d'identité, à savoir via :

- un microprocesseur électronique, qui contient toutes les informations lisibles de manière électronique et qui sont énumérées dans la loi
- un code-barres au sujet duquel on ne sait pas clairement quelles informations lisibles de manière électronique il contient.

21. L'arrêté royal (arrêté d'exécution) fait uniquement mention d'un microprocesseur électronique. L'Autorité constate que la modification envisagée vise à légaliser une pratique déjà d'application. Les cartes d'identité actuelles contiennent déjà un tel code-barres, sans que cela ait été spécifié dans la réglementation et sans qu'il ne soit précisé quelles informations ce code-barres contient. Le demandeur a fait savoir que derrière le code-barres, se cachent les informations suivantes : le numéro de Registre national, le numéro de carte, la durée de validité et la date de naissance. Dans un souci de clarté et de transparence, ceci doit au moins être précisé dans l'arrêté royal.

22. Selon les informations complémentaires fournies par le demandeur, la finalité en vue de laquelle un code-barres est prévu est double :

- le contrôle des données qui sont imprimées sur la carte (l'Autorité en déduit que le but est de détecter une éventuelle manipulation des données imprimées sur la carte) ;
- l'accès rapide à un nombre limité de données lorsqu'une lecture avec le lecteur de carte n'est pas possible.

23. La question se pose de savoir si l'apposition d'un code-barres constitue un moyen efficace pour atteindre la première finalité : si l'on parvient à manipuler l'impression des données sur la carte d'identité, rien n'empêche que l'on manipule aussi ce code-barres.

24. On n'a pas besoin d'un code-barres pour accéder rapidement à certaines informations mentionnées sur la carte d'identité. Les informations qui se cachent derrière le code-barres sont imprimées sur la carte et peuvent donc être consultées immédiatement (= rapidement) *de visu*. Dans la mesure où le but est par exemple de contrôler l'âge lorsqu'on souhaite obtenir quelque chose d'un distributeur automatique (cigarettes, alcool), il suffit que l'âge soit mentionné sous la forme d'un code-barres.

25. L'Autorité ne peut pas s'empêcher de penser que le but du code-barres consiste à collecter rapidement des informations de manière électronique concernant des personnes, alors qu'on ne sait pas clairement à qui cet équipement est destiné ni pourquoi ces informations sont collectées. Si tel est le cas, cela doit être précisé.

26. Un accès rapide à un ensemble limité de données est également intéressant d'un point de vue commercial. Un citoyen peu soupçonneux qui présente sa carte d'identité, par exemple pour prouver qu'il satisfait à l'exigence d'âge pour acquérir un bien déterminé, ne verra pas d'inconvénient à ce que le commerçant passe sa carte d'identité au scanner de codes-barres car il n'a pas conscience que ses données à caractère personnel sont ainsi lues. Il n'a aucune garantie que lors du scannage du code-barres, les données qui y figurent ne sont pas enregistrées. À l'aide des données qui peuvent ainsi être recueillies, on peut déjà aller assez loin sur Internet pour se faire passer pour quelqu'un que l'on n'est pas : on dispose du numéro de Registre national, du numéro de la carte d'identité et de la date de naissance, c'est-à-dire des données qui sont fréquemment utilisées par des sites Internet pour identifier une personne.

27. Le risque que le code-barres favorise une fraude à l'identité sur Internet est donc réel et donc contraire à l'objectif poursuivi par l'opération. Dans l'AIPD qui a été fournie, aucune attention n'a été accordée à cet aspect, malgré les conséquences potentiellement préjudiciables pour les droits et libertés de la personne concernée.

D.3. Capteur ad hoc

28. Le projet complète l'article 3 de l'arrêté royal avec un nouveau paragraphe 5. Le deuxième alinéa de ce paragraphe précise ce qui suit : *"Les empreintes digitales sont numérisées à l'initiative de l'officier de l'état civil ou de son délégué au moyen de capteurs ad hoc.*

L'image numérisée des empreintes est transmise par le biais des services du Registre national au producteur de la carte d'identité, afin d'y être intégrée dans celle-ci.".

29. En ce qui concerne cette problématique, il est fait référence au rapport d'analyse technique en annexe.

D.4. Absence de mention des données légalement prescrites

30. La loi dispose que la carte d'identité contient la signature du titulaire. L'article 3, § 3 de l'arrêté royal précise que si le titulaire ne peut pas signer, en raison de son analphabétisme, d'un handicap ou d'une maladie, la signature est remplacée par la mention "dispensé". Actuellement, cette preuve est fournie au moyen d'un "certificat récent" (sauf lorsque c'est manifestement visible). En vertu de l'article 3, 6° du projet, les termes "certificat récent" sont remplacés par "**certificat médical** daté de moins d'un mois".

31. Par conséquent, des catégories particulières de données à caractère personnel au sens de l'article 9 du RGPD seront incontestablement traitées, sans qu'on ait la moindre idée d'un certain nombre d'éléments essentiels du traitement, comme :

- qui est le responsable du traitement : s'agit-il de l'officier de l'état civil (et par extension la commune) qui prend la décision sur la base du certificat ? Ou le Ministre de l'Intérieur/le SPF Intérieur tranche-t-il ? ;
- le certificat est-il conservé à la commune ou est-il transmis au Ministre de l'Intérieur/SPF Intérieur pour y être conservé ? ;
- combien de temps sont conservées les informations et pour quelles raisons ?

32. Pour ce traitement, le demandeur doit identifier un fondement du traitement sur la base de l'article 9.2 du RGPD.

33. L'article 6, § 2, troisième alinéa de la loi du 19 juillet 1991 stipule que l'empreinte digitale de l'index de la main gauche et de la main droite est enregistrée ou, en cas d'inaptitude, d'un autre doigt de chaque main, le Roi déterminant les modalités.

34. Comme déjà précisé, le projet complète l'article 3 de l'arrêté royal avec un nouveau paragraphe 5. Les alinéas 4 à 7 de ce paragraphe régissent les cas dans lesquels une carte d'identité ou une carte d'étranger ne comportant pas d'empreintes digitales est délivrée, et ce alors que la loi ne prévoit pas que des cartes d'identité ne comportant pas d'empreintes digitales puissent être délivrées et ne prévoit pas non plus de délégation au Roi.

35. Vu que l'Autorité n'est pas favorable à l'enregistrement d'empreintes digitales sur la carte d'identité, prévoir des situations dans lesquelles aucune empreinte digitale n'est enregistrée n'est donc en soi pas problématique d'un point de vue du traitement de données. Cela n'empêche pas que le régime de cartes d'identité "**sans empreintes digitales**" élaboré par le projet puisse quand même donner lieu à plusieurs réserves.

36. Une carte d'identité ne comportant pas d'empreintes digitales sera délivrée lorsque le titulaire :

- ne peut pas fournir ses empreintes digitales en raison d'un handicap physique ou d'une maladie, de façon permanente ou pendant une durée de plus de 3 mois. La preuve est apportée au moyen d'un certificat médical, sauf lorsqu'il est manifeste que la personne concernée n'est pas à même de donner ses empreintes digitales en raison d'un handicap ou d'une maladie clairement visible ;
- ne peut pas donner des empreintes digitales de qualité suffisante pour être capturées, en raison d'une particularité physique. Il appartient à l'agent communal d'apprécier cette impossibilité ;
- ne peut pas se déplacer pour fournir ses empreintes digitales, de façon permanente ou pendant une durée de plus de 3 mois. La preuve est apportée au moyen d'un certificat médical ;
- se trouve dans l'impossibilité de se déplacer pendant une durée de plus de 3 mois pour fournir ses empreintes digitales en raison d'une décision judiciaire. La preuve est apportée au moyen d'une copie de cette décision judiciaire.

37. Si l'on examine les chiffres cités au Parlement lors du traitement du projet de loi instaurant les empreintes digitales sur la carte d'identité, on ne peut que constater que le nombre de cas de fraude à l'identité à l'aide de la carte d'identité et de fraude fondée sur la ressemblance est très restreint (le ministre compétent a fourni au Parlement les chiffres suivants : fraude à l'identité constatée à l'aide d'une carte d'identité en 2018 : 566 ; fraude fondée sur la ressemblance : 159 cas pendant le premier semestre 2018[5] - à titre de précision, environ 11 millions de cartes d'identité et de cartes d'étranger sont en circulation).

38. L'Autorité est toutefois consciente que la fraude à l'identité ne constitue généralement qu'un élément de l'intention criminelle plus large. Les exceptions formulées ci-dessus offrent néanmoins des perspectives intéressantes pour les personnes qui ont l'intention de commettre une fraude et souhaitent à cette fin être en possession d'une carte d'identité "sans empreintes digitales".

[5] Chambre, doc 54 - 3256/003 - p. 31-34.

39. Dans 2 cas, la preuve de l'impossibilité de fournir des empreintes digitales peut être apportée au moyen d'un **certificat médical**. Il y a régulièrement des vols de certificats médicaux vierges, qui sont vendus et peuvent ensuite être complétés à discrétion. Ils peuvent également être falsifiés assez facilement. Comment l'agent communal auquel un tel certificat est soumis pourra-t-il établir s'il s'agit d'un certificat de bonne foi ?

40. Par souci d'exhaustivité, en ce qui concerne la problématique du certificat médical, l'Autorité renvoie aux remarques formulées au point 31.

41. L'**agent communal** est habilité à **apprécier** la particularité physique qui empêche de fournir des empreintes digitales de qualité suffisante pour être capturées. Cette définition laisse une large compétence d'appréciation à l'agent communal et donc la possibilité, pour des personnes malintentionnées, d'anticiper en menaçant par exemple un fonctionnaire. En outre, on ne sait pas clairement si une telle décision est enregistrée et si oui, où ? On ne sait pas non plus clairement si cette décision est documentée et si oui, où et combien de temps ces informations sont-elles conservées ? Étant donné les circonstances, l'Autorité ne peut pas juger si cela engendre un traitement de données à caractère personnel supplémentaire ni qui doit être qualifié de responsable du traitement dans ce cadre. Cela doit donc être précisé.

42. Une personne qui, à la suite d'une décision judiciaire, se trouve dans l'impossibilité de se déplacer pendant une période de plus de 3 mois pour fournir ses empreintes digitales est également dispensée. Selon les informations complémentaires reçues le 15/03/2019, on vise ainsi notamment les détenus. Concrètement, cela signifie donc qu'une personne qui a été condamnée à une peine d'emprisonnement de 5 ans et dont la carte d'identité doit être renouvelée dans le courant de la 4e année de sa peine d'emprisonnement recevra une carte d'identité ne comportant pas d'empreintes digitales alors que des citoyens qui n'ont jamais encouru aucune condamnation doivent quant à eux bel et bien transmettre leurs empreintes digitales.

43. Des cartes d'identité ne comportant pas d'empreintes digitales seront donc en circulation. L'Autorité propose que l'arrêté royal prévoie un régime analogue à celui prévu en l'absence d'une signature sur la carte d'identité, à savoir que les empreintes digitales soient remplacées par la mention "dispensé". Il est recommandé d'apposer une telle mention sécurisée sur la puce où doivent normalement figurer les empreintes digitales.

E. Personnes concernées

44. Elles sont définies à l'article 6, premier alinéa de la loi du 19 juillet 1991. Il s'agit des Belges et des étrangers inscrits aux registres de la population.

F. Entités auxquelles les données à caractère personnel peuvent être communiquées et finalités pour lesquelles elles peuvent l'être

45. En ce qui concerne les empreintes digitales, l'article 6, § 2, sixième alinéa de la loi du 19 juillet 1991 définit les entités qui peuvent lire les empreintes digitales ainsi que les finalités pour lesquelles elles peuvent le faire. Dans un certain nombre de cas, il est fait mention de "lutte contre la fraude", entendez lutte contre la fraude à l'identité.

46. La règle de base est claire : les entités visées peuvent uniquement "lire". Cela signifie que l'enregistrement des empreintes digitales doit être conçu de telle manière à ce qu'elles ne puissent pas être copiées électroniquement, ni lues par un appareil qui n'est pas spécifiquement destiné à cet effet. Cela ne ressort pas des documents fournis par le demandeur.

47. L'Autorité constate que le simple fait de lire et donc d'examiner les empreintes digitales figurant sur la carte ne suffira pas à vérifier si les empreintes digitales de la personne qui se présente avec une carte sont les mêmes que celles figurant sur la carte. Il est nécessaire que la personne concernée place ses doigts dans un "lecteur" et qu'une comparaison soit ensuite effectuée entre l'image sur la carte et l'image sur le lecteur. Il faut donc, quoi qu'il en soit, faire plus que simplement "lire" les empreintes digitales.

G. Durée de conservation

48. Plusieurs données mentionnées sur la carte d'identité sont enregistrées dans le Registre des cartes d'identité dont le délai de conservation est régi légalement. Les empreintes digitales ne sont pas enregistrées dans ce registre. La durée de conservation de ces empreintes - en dehors de la carte d'identité - est légalement fixée à 3 mois, délai dans lequel la carte d'identité doit normalement pouvoir être fabriquée (article 6, § 2 de la loi du 19 juillet 1991). C'est le responsable du traitement qui assure le contrôle de cette obligation. Qui est le responsable du traitement qui doit veiller au respect de cette disposition ? Ni la loi, ni le projet ne fournissent des précisions à cet égard (voir également le point 8).

49. Le SPF Intérieur assure le stockage central des empreintes digitales pendant une période de 3 mois. L'Autorité déduit de l'AIPD (p. 7) que les empreintes digitales, avec toutes les autres données

mentionnées sur la carte d'identité, sont également conservées pendant un mois auprès du producteur des cartes. Cela signifie qu'un grand nombre de données, des données particulières (article 9 du RGPD), sont stockées à deux endroits, ce qui augmente considérablement le risque d'une violation de données à caractère personnel. En page 8 de l'AIPD, on lit que "*Il est prévu d'organiser, à court terme, un contrôle d'effectivité des effacements.*". Si jusqu'à présent, aucun contrôle n'a eu lieu quant aux effacements des données que les sous-traitants ont reçues en vue de la fabrication des cartes d'identité, ce n'est pas particulièrement rassurant.

50. Étant donné que la durée de validité de la carte d'identité est de 10 ans, les empreintes digitales sont conservées sur ce support pendant 10 ans. Pendant cette période, le titulaire de la carte a le contrôle des informations qu'elle contient, dans le cadre réglementairement établi. Lorsque la durée de validité de la carte expire, ce dernier la remettra à un fonctionnaire compétent de la commune, lors de la délivrance de sa nouvelle carte d'identité.

51. Actuellement, on ne sait pas clairement ce qu'il advient ensuite de la carte d'identité qui a été rendue. Est-elle détruite par la commune ? Si oui, quand est-elle détruite et de quelle façon ? La destruction est-elle confiée à des tiers ? Ces cartes d'identité qui ont été rendues sont-elles collectées de manière centralisée et détruites ensuite ? Si oui, par qui ? Quand sont-elles détruites et de quelle façon ?

52. Cet aspect doit être réglé de manière claire. L'Autorité estime que, vu le caractère très intrusif des empreintes digitales sur la carte d'identité, on peut exiger que la carte d'identité qui a été rendue soit détruite en présence de son titulaire.

H. Autres remarques

H.1. Moment de l'enregistrement des empreintes digitales sur la carte d'identité

53. Le premier alinéa du nouveau § 5 de l'article 3 dispose que le Ministre ayant l'Intérieur dans ses attributions fixe la date à laquelle les cartes d'identité et les cartes d'étranger doivent comporter les empreintes digitales. Le Ministre ayant les Affaires étrangères dans ses attributions fait la même chose pour les cartes d'identité de Belges à l'étranger visées à l'article 39 du *Code consulaire*.

54. Conformément à l'article 39 du *Code consulaire*, la carte d'identité délivrée par le poste consulaire présente "*des caractéristiques identiques*" à celles de la carte d'identité délivrée à un Belge en Belgique[6]. Ni le Code consulaire, ni l'arrêté royal du 19 avril 2014 *relatif aux cartes d'identité*

[6] Ceci est d'ailleurs également explicitement souligné par l'article 6, § 1er, troisième alinéa de la loi du 19 juillet 1991.

délivrées par les postes consulaires de carrière ne contiennent actuellement la moindre des précisions requises en vertu de l'article 6.3 du RGPD. Ce code/cet arrêté devra donc être adapté en vue de la délivrance de cartes d'identité comportant des empreintes digitales.

55. L'Autorité souligne la nécessité d'effectuer au préalable une analyse d'impact relative à la protection des données approfondie (article 35.3.b) du RGPD). Il s'agit de la collecte à grande échelle de données sensibles présentant un risque élevé pour les droits et libertés des personnes concernées, par des acteurs répartis dans le monde entier, et qui sont ensuite transmises notamment à un sous-traitant en vue de la fabrication de la carte d'identité.

H.2. Article 4 du projet (insère un article 3/1)

56. Un citoyen ne recevra *de facto* sa nouvelle carte qu'après que l'agent communal aura comparé aussi bien la photographie que les empreintes digitales sur la carte avec le visage et les empreintes digitales de la personne qui se présente.

57. Vu que des cartes d'identité ne comportant pas d'empreintes digitales sont délivrées, il est recommandé, en ce qui concerne les empreintes digitales, de préciser peut-être "dans la mesure où des empreintes digitales ont été enregistrées sur la carte".

H.3. Article 6 du projet (remplace l'actuel article 6 de l'arrêté royal)

58. L'article 6*ter* de la loi du 19 juillet 1991 précise qu'en cas de perte, vol ou destruction, une déclaration est faite auprès de l'administration communale, de la police ou du Helpdesk du Registre national en ce qui concerne la carte d'identité d'un Belge et auprès de la police en ce qui concerne la carte d'étranger. Lors de la déclaration, une attestation est délivrée. L'article 6 du projet détaille cette disposition.

59. En ce qui concerne la carte d'identité :

- auprès de l'administration communale du lieu de sa résidence principale pendant les heures de bureau (§ 1er, premier alinéa). L'administration fournit une attestation de perte, vol ou destruction et charge le prestataire de service de certification de retirer les fonctions électroniques de la carte de telle sorte que ces fonctions soient définitivement mises hors service et annule la carte d'identité ;
- auprès du Helpdesk du Registre national qui retire les fonctions électroniques. La personne concernée doit alors encore se rendre à la commune pour obtenir une attestation et l'annulation de la carte d'identité ;

- auprès de la police en dehors des heures de bureau ou si l'administration communale est inaccessible. La police fournit l'attestation et en transmet une copie au Helpdesk du Registre national en vue du retrait des fonctions électroniques et ce dernier avertit ensuite la commune afin qu'elle annule la carte.

60. En ce qui concerne la carte d'étranger, la déclaration se fait toujours auprès de la police. La police fournit l'attestation et en transmet une copie au Helpdesk du Registre national en vue du retrait des fonctions électroniques et ce dernier avertit ensuite la commune afin qu'elle annule la carte.

61. Pour une bonne compréhension : lorsque dans le texte, on parle des fonctions électroniques de la carte qui sont retirées, cela signifie concrètement la mise hors service des certificats. Les informations lisibles de manière électronique sur une carte perdue ou volée resteront lisibles de manière électronique.

62. Le Helpdesk du Registre national reçoit de la police une copie de l'attestation de perte, vol ou destruction de la carte[7] de manière à pouvoir désactiver les fonctions électroniques. Vu qu'il ne faut pas perdre de temps pour le retrait des certificats, l'Autorité suppose qu'une copie de cette attestation est transmise au Helpdesk du Registre national par voie électronique. Les articles 5.1.f), 24.1 et 32 du RGPD mentionnent explicitement l'obligation pour le responsable du traitement de prendre les mesures techniques et organisationnelles appropriées qui sont requises pour protéger les données à caractère personnel. Ces mesures doivent assurer un niveau de sécurité approprié, compte tenu, d'une part, de l'état des connaissances en la matière et des coûts qu'entraîne l'application de ces mesures et, d'autre part, de la nature des données à protéger et des risques potentiels. À défaut de la moindre information concernant la manière dont cette communication a lieu, l'Autorité exprime l'espoir que la transmission des copies des attestations se fait via un canal sécurisé et pas simplement par e-mail. L'utilisation de ce dernier moyen est en effet problématique à la lumière des éléments précités. La copie de l'attestation équivaut, pour le Helpdesk du Registre national, à la mission de désactiver les certificats. En cas de discussion ou de contestation, le Helpdesk dispose également d'une preuve. Il n'est précisé nulle part ce que le Helpdesk du Registre national fait avec ces copies, ni combien de temps celles-ci sont conservées. À la lumière de l'article 5.1.e) du RGPD, ceci doit être précisé dans l'arrêté.

63. Le nouvel article 6, § 5 de l'arrêté royal tel que proposé prévoit qu'une carte d'identité ou une carte d'étranger qui est retrouvée doit être restituée à l'administration communale, que le titulaire ait déjà reçu une nouvelle carte ou non. Selon l'arrêté royal actuel, une carte retrouvée ne doit être restituée que lorsqu'elle a été retrouvée après avoir été renouvelée.

[7] Dans le nouvel article 6, § 4 de l'arrêté royal tel que proposé, il est fait mention d'un modèle d'attestation. Selon les informations complémentaires reçues le 20/03/2019, il s'agit d'un renvoi au modèle qui a été annexé à l'actuel arrêté royal.

64. Il n'est pas précisé ce qu'il advient de la carte restituée. Un accusé de réception est-il remis à celui qui restitue la carte ? Après réactivation des certificats, est-elle restituée au titulaire s'il n'a pas encore reçu de nouvelle carte ? La carte est-elle détruite par la commune et comment cela se passe-t-il ? Les cartes sont-elles transmises au Registre national qui se charge de la destruction ? La destruction d'office est-elle documentée et enregistrée ? Ceci doit être précisé dans l'arrêté (voir également les points 51-52).

J. Synthèse technique

65. Sur la base de l'AIPD reçue par l'Autorité, une analyse technique qui soulève de très nombreuses questions, tant au niveau de la sécurité qu'au niveau de l'intégrité du processus, a été réalisée (voir l'annexe confidentielle).

66. L'Autorité souhaite toutefois formuler les réserves suivantes.

67. Quant à l'information sur la technologie de la puce utilisée, dans le document reçu, il est mentionné l'utilisation d'une mémoire ROM (Read Only Memory) Or, dans ce type de technologie, le contenu de la mémoire est inséré lors de la fabrication. Un doute est émis sur l'utilisation d'une ROM au niveau de la puce RFID. Nous pensons qu'il s'agit plutôt d'EEPROM (Electrically Erasable Programmable Read Only Memory) qui sont donc effaçables et reprogrammables électriquement.

68. Il est fait mention, dans les informations reçues, des prescriptions et recommandations de l'ICAO dans le cadre de MRTD (Machine Readable Travel Document) alors que dans ce cas-ci, il est question de eMRTDs (electronic Machine Readable Travel Documents). Il y est bien fait référence au Doc 9303 Septième Édition, 2015 Partie 1, Partie 3 et Partie 5 de ICAO dans les normes, mais aucune trace de la Partie 11 du Doc 9303 traitant des Mécanismes de sécurité pour le MRTDs et plus particulièrement des mesures supplémentaires à envisager dans le cadre des eMRTDs. En effet, cette Partie 11 fournit des spécifications pour permettre aux États et aux fournisseurs de mettre en œuvre les fonctions de sécurité cryptographiques pour documents de voyage électroniques lisibles à la machine ("eMRTDs") avec circuit intégré (puce électronique) sans contact. Les protocoles cryptographiques sont spécifiés pour :

- empêcher les attaques par "skimming" (écrèmage) des données présentes sur les puces RFID
- empêcher les attaques par "eavesdropping" (l'interception illicite de communications) entre la puce sur la carte et le lecteur
- assurer l'authentification des données stockées dans la puce sans contact sur la base de l'infrastructure à clés publiques (ICP) décrite dans la Partie 12 du Doc 9303 (non évoquée non plus)
- assurer l'authentification de la puce sans contact.

Il est à remarquer que la présente édition du Doc 9303 ne spécifie aucun contrôle d'accès supplémentaire aux données sensibles (c'est-à-dire les éléments biométriques secondaires), c'est-à-dire la photo et les empreintes digitales, mais que l'emploi de mécanismes nationaux pour protéger ces données est autorisé. Il est prévu d'inclure une spécification interopérable à cette fin dans les futures versions du Doc 9330. Aucune information n'est donnée sur les mécanismes que la Belgique compte mettre en place pour protéger l'accès à ces informations. Le tableau reprend les différentes options possibles avec, en bleu, les mesures supposées retenues pour la nouvelle eID.

69. Les mesures de protection n'empêchent pas la copie exacte ni le remplacement de la puce. Ceci pose un problème d'intégrité du document et ne garantit donc pas l'authenticité.

70. Les mesures qui mitigent les nouveaux risques introduits par l'utilisation des puces sans contact (RFID), à s'avoir l'écrémage et l'interception des communications, reposent sur la cryptographie.
Or, les points faibles des mesures cryptographiques posent deux questions : Que fait-on si les clés sont découvertes ? Scénario envisageable soit en cas de vol des clés, soit en cas d'augmentation de la puissance de calcul disponible suite à l'évolution des technologies. Quelles seront les possibilités technologiques dans 10 ans ? Les algorithmes et les longueurs de clés utilisés, les certificats envisagés aujourd'hui seront-t-ils encore fiables dans 10 ans au vu de la rapidité d'évolution de la technologie, principalement la puissance de calcul que nous proposeront les calculateurs quantiques ?

PAR CES MOTIFS,
l'Autorité

↳ estime que les adaptations suivantes s'imposent :

- préciser qui sont les responsables (conjoints)/sous-traitants (points 7 et 8) ;
- accroître le contrôle du citoyen sur ses données au moyen de mesures techniques appropriées (points 17-19) ;
- préciser les informations qui se cachent derrière le code-barres (point 21) ;
- réexaminer l'utilité et la sécurité du code-barres dans sa forme actuelle (points 25-27) ;
- en ce qui concerne les certificats médicaux qui sont fournis en vue d'une dispense de signature et d'empreintes digitales, préciser le fondement juridique, qui est le responsable du traitement et combien de temps ces certificats sont conservés (points 31 et 40) ;
- prévoir des mesures pour prévenir l'abus du régime de dispense (points 39 et 41) ;
- concernant les décisions accordant une dispense d'empreintes digitales, préciser qui est le responsable du traitement, combien de temps elles sont conservées (point 41) ;

- apposer la mention "dispensé" sur la puce d'une carte d'identité/carte d'étranger ne comportant pas d'empreintes digitales (point 43) ;
- régler explicitement la destruction de la carte d'identité/carte d'étranger (points 51-52) ;
- en ce qui concerne les cartes d'identité délivrées par des ambassades et des postes consulaires, la réglementation doit être adaptée (point 54) et une AIPD doit être réalisée (point 55) ;
- préciser combien de temps la copie de l'attestation de perte, vol ou destruction est conservée par le Helpdesk du Registre national (point 62) ;
- préciser ce qu'il advient de la carte d'identité/carte d'étranger qui est restituée après avoir été déclarée volée ou perdue (point 64) ;

↳ attire l'attention sur les aspects suivants :

- il est recommandé de réexaminer la technologie utilisée de la puce (points 18, 67-70) ;

- avant d'entamer la production, tout le processus relatif à la fabrication de la carte d'identité doit être profondément réexaminé en fonction des constatations figurant dans l'analyse technique réalisée par l'Autorité (point 65) ;

- le simple fait de "lire" les empreintes digitales comme cela est prévu dans la loi ne permet pas de procéder à une comparaison (point 47).

(sé) An Machtens
Administrateur f.f.,

(sé) Willem Debeuckelaere
Président,
Directeur du centre de connaissances