DOC 55 **3961/002**

CHAMBRE DES REPRÉSENTANTS
DE BELGIQUE

15 avril 2024

# PROJET DE LOI

## modifiant la loi du 15 août 2012 relative à la création et à l'organisation d'un intégrateur de services fédéral

## Avis de l'Autorité de protection des données

**Sommaire** Pages



*Voir:*

Doc 55 **3961/ (2023/2024)**:
001: Projet de loi.

BELGISCHE KAMER VAN
VOLKSVERTEGENWOORDIGERS

15 april 2024

# WETSONTWERP

## tot wijziging van de wet van 15 augustus 2012 houdende oprichting en organisatie van een federale dienstenintegrator

## Advies van de Gegevensbeschermingsautoriteit

**Inhoud** Blz.



*Zie:*

Doc 55 **3961/ (2023/2024)**:
001: Wetsontwerp.

| | | |
|---|---|---|
| *N-VA* | : | *Nieuw-Vlaamse Alliantie* |
| *Ecolo-Groen* | : | *Ecologistes Confédérés pour l'organisation de luttes originales – Groen* |
| *PS* | : | *Parti Socialiste* |
| *VB* | : | *Vlaams Belang* |
| *MR* | : | *Mouvement Réformateur* |
| *cd&v* | : | *Christen-Democratisch en Vlaams* |
| *PVDA-PTB* | : | *Partij van de Arbeid van België – Parti du Travail de Belgique* |
| *Open Vld* | : | *Open Vlaamse liberalen en democraten* |
| *Vooruit* | : | *Vooruit* |
| *Les Engagés* | : | *Les Engagés* |
| *DéFI* | : | *Démocrate Fédéraliste Indépendant* |
| *INDEP-ONAFH* | : | *Indépendant - Onafhankelijk* |

| *Abréviations dans la numérotation des publications:* | | *Afkorting bij de nummering van de publicaties:* | |
|---|---|---|---|
| *DOC 55 0000/000* | *Document de la 55e législature, suivi du numéro de base et numéro de suivi* | *DOC 55 0000/000* | *Parlementair document van de 55e zittingsperiode + basisnummer en volgnummer* |
| *QRVA* | *Questions et Réponses écrites* | *QRVA* | *Schriftelijke Vragen en Antwoorden* |
| *CRIV* | *Version provisoire du Compte Rendu Intégral* | *CRIV* | *Voorlopige versie van het Integraal Verslag* |
| *CRABV* | *Compte Rendu Analytique* | *CRABV* | *Beknopt Verslag* |
| *CRIV* | *Compte Rendu Intégral, avec, à gauche, le compte rendu intégral et, à droite, le compte rendu analytique traduit des interventions (avec les annexes)* | *CRIV* | *Integraal Verslag, met links het definitieve integraal verslag en rechts het vertaalde beknopt verslag van de toespraken (met de bijlagen)* |
| *PLEN* | *Séance plénière* | *PLEN* | *Plenum* |
| *COM* | *Réunion de commission* | *COM* | *Commissievergadering* |
| *MOT* | *Motions déposées en conclusion d'interpellations (papier beige)* | *MOT* | *Moties tot besluit van interpellaties (beigekleurig papier)* |

Autorité de protection des données
Gegevensbeschermingsautoriteit

**Avis n° 24/2024 du 18 mars 2024**

**Objet: Avant-projet de loi modifiant de la loi relative à la création et à l'organisation d'un intégrateur de services fédéral (CO-A-2023-554)**

**Version originale**

Le Centre de Connaissances de l'Autorité de protection des données (ci-après « l'Autorité »),
Présent.e.s : Mesdames Juline Deschuyteneer, Cédrine Morlière, Nathalie Ragheno et Griet Verhenneman et Messieurs Yves-Alexandre de Montjoye, Bart Preneel et Gert Vermeulen;

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 « LCA »);

Vu l'article 25, alinéa 3, de la LCA selon lequel les décisions du Centre de Connaissances sont adoptées à la majorité des voix ;

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* (ci-après « 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 « LTD »);

Vu la demande d'avis du Secrétaire d'État à la Digitalisation, chargé de la Simplification administrative, de la Protection de la vie privée et de la Régie des bâtiments, adjoint au Premier ministre, Monsieur Mathieu Michel (ci-après « le demandeur »), reçue le 7 décembre 2023;

Vu la transmission de la demande d'avis par l'Autorité, le 12 janvier 2024, à l'Organe de contrôle de l'information policière (le COC), au Comité permanent de contrôle des services de renseignement (le CPR) et au Comité permanent de contrôle des services de police (le CPP), conformément à l'article

54/1 de la LCA et au Protocole de coopération entre les autorités de contrôle fédérales belges en matière de protection des données, conclu le 24 novembre 2020;

Vu la réponse communiquée par le COC le 7 février 2024, selon laquelle celui-ci ne rendra pas d'avis;

Vu l'absence de confirmation du CPR à la date de rédaction du présent avis quant à la question de savoir s'il rendra un avis;

Vu l'absence de confirmation du CPP à la date de rédaction du présent avis quant à la question de savoir s'il rendra un avis;

Émet, le 18 mars 2024, l'avis suivant :

## I. Objet et contexte de la demande d'avis

1. Le demandeur a introduit auprès de l'Autorité une demande d'avis concernant un avant-projet de loi *modifiant la loi relative à la création et à l'organisation d'un intégrateur de services fédéral* (CO-A-2023-554) (ci-après, « **le Projet** »). Le Projet modifie la loi du 15 août 2012 *relative à la création et à l'organisation d'un intégrateur de services fédéral* (ci-après, « **la loi de 2012** »).

2. L'exposé des motifs du Projet explique que son objectif est notamment de tenir compte de la modification d'autres législations, d'apporter des améliorations à la loi de 2012 découlant de la pratique et des enseignements tirés et d'intégrer à celle-ci la terminologie du RGPD. Le Projet entend clarifier certaines définitions et établir les rôles de l'intégrateur de services, des services publics participants et des sources authentiques de données au regard du traitement de données à caractère personnel.

3. Le Projet s'inscrit également pour partie dans le droit européen. Ainsi, il « *tient compte* » du Règlement (UE) n° 2022/868 du Parlement européen et du Conseil du 30 mai 2022 *portant sur la gouvernance européenne des données et modifiant le règlement (UE) 2018/1724 (règlement sur la gouvernance des données)* (ci-après, « **le Règlement sur la Gouvernance des Données** » ou « DGA »), afin de permettre à l'intégrateur de services fédéral de contribuer à ce dispositif. Il clarifie également une mission de l'intégrateur de service dans ce contexte.

4. Il « *complète* » la Directive (UE) n° 2019/1024 du Parlement européen et du Conseil du 20 juin 2019 *concernant les données ouvertes et la réutilisation des informations du secteur public (refonte)* (ci-après, « **la Directive réutilisation** ») et compte-tenu du fait qu'actuellement « *l'intégrateur de service fédéral fournit le portail où les données ouvertes sont publiées* », il « *ancre la mise à disposition par l'intégrateur de services fédéral de ce type d'information* ».

5. Par ailleurs, le Projet **anticipe également sur la réforme en cours** 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* (ci-après, « **le Règlement eIDAS** »), en ce qui concerne les « *portefeuilles d'identité numérique* ». Il est encore relatif au Règlement eIDAS et à la loi du 18 juillet 2017 relative à l'identification électronique (ci-après, « **la loi eIDAS** ») tels que ces normes existent en droit positif.

6. Enfin, il exécute également le Règlement (UE) n° 2018/1724 du Parlement européen et du Conseil du 2 octobre 2018 *établissant un portail numérique unique pour donner accès à des informations, à des procédures et à des services d'assistance et de résolution de problèmes, et modifiant le règlement (UE) n° 1024/2012* (ci-après, « **le Règlement 2018/1724** »).

## II. Examen

Le présent avis est structuré comme suit :

## II.1. Avis pertinents de l'Autorité, portée du Projet et portée du présent avis

7. Dans plusieurs avis récents, l'Autorité a eu l'occasion de rappeler sa pratique d'avis dans le domaine de l'échange de données issues de sources authentiques (ou non). Il convient par conséquent de se référer à titre préliminaire **aux avis suivants de l'Autorité** :

   - L'avis n° 154/2023 du 20 octobre 2023 *concernant un avant-projet de décret et ordonnance conjoints portant le code bruxellois de la gouvernance et de la donnée (CO-A-2023-407)* (en particulier, les considérants nos 46-72) (ci-après, « **l'avis n° 154/2023** ») ;

   - L'avis n° 143/2023 du 29 septembre 2023 *concernant un avant-projet de décret portant assentiment à l'accord de coopération entre la Région wallonne et la Communauté française désignant l'intégrateur de services de la Région wallonne et de la Communauté française et un projet d'accord de coopération relatif à la création du service commun aux Gouvernements Wallon et de la Communauté française, dénommé Banque Carrefour d'échange de données (non soumis à assentiment) (CO-A-2023-375), et concernant un avant-projet de décret portant assentiment à l'accord de coopération entre la Région wallonne et la Communauté française désignant l'intégrateur de services de la Région wallonne et de la Communauté française et un projet d'accord de coopération relatif à la création du service commun aux Gouvernements Wallon et de la Communauté française, dénommé Banque Carrefour d'échange de données (non soumis à assentiment) (CO-A-2023-376)* (ci-après, « **l'avis n° 143/2023** »).

8. L'Autorité observe que le Projet **modifie substantiellement la loi de 2012 qui constitue le dispositif central de droit fédéral relatif, notamment, aux sources authentiques de**

**données**. Comme le Conseil d'Etat l'indique dans son avis[1], en déplorant la saisine concomitante de l'Autorité, ce projet « *concern*[e] *par excellence le traitement de données à caractère personnel* ». En particulier :

- Le Projet étend significativement le champ d'application *ratione personae* de la loi de 2012 en abandonnant le concept de « *service public participant* » au profit de celui, beaucoup plus large, d' « *utilisateur* » ;

- Il modifie le concept de « *source authentique de données* »[2] ainsi que les règles selon lesquelles des sources de données sont qualifiées comme telles ;

- Il attribue de nouvelles missions à l'intégrateur de services fédéral dont les services pourront en outre, être accessibles aux Communautés, Régions, pouvoirs locaux et organismes en dépendant ;

- Il porte sur la responsabilité de l'intégrateur de services fédéral, de ses utilisateurs, ainsi que sur les droits des personnes concernées dans ce contexte ;

- Il ne clarifie pas la portée de certaines dispositions importantes de la loi de 2012 qui manquent pourtant de clarté, telles que les dispositions relatives au caractère non contraignant du recours aux services de l'intégrateur de services fédéral ;

- Enfin, le Projet exécute des dispositions de droit européen et anticipe sur l'exécution de règles européennes qui ne sont pas encore adoptées (le Projet étant lui-même changeant sur ce point[3]).

9. Dans ce contexte, l'Autorité a interrogé le demandeur quant à la réalisation d'une **analyse d'impact relative à la protection des données**. Celui-ci a répondu ce qui suit :

> « ***Aucune analyse d'impact en matière de protection des données n'a été réalisée suite à la rédaction du projet même de modification de la loi.***
> *Les modifications mentionnées auront bien sûr un impact sur le traitement des données à caractère personnel par l'intégrateur de services. Le SPF BOSA attache la plus grande importance à la protection des personnes physiques en ce qui concerne le traitement des*

[1] C.E., avis n° 75.185/2 du 13 février 2024 sur un '*avant-projet de loi modifiant la loi relative à la création et à l'organisation d'un intégrateur de services fédéral*.

[2] Même si, au cours de la mise en état du dossier, le demandeur a renoncé à modifier ce concept.

[3] Voir la réponse communiquée par le demandeur et reprise au considérant n° 14.

*données à caractère personnel. Le traitement effectif des données à caractère dans le cadre de l'extension des catégories d'utilisateurs, de l'extension des sources authentiques possibles et des nouvelles missions fera donc l'objet d'évaluations d'impact en matière de protection des données, telles que requises en vertu de l'article 35 du RGPD* » (mis en gras par l'Autorité).

10. Compte-tenu de la portée du Projet[4], **l'Autorité est d'avis que celui-ci devrait être accompagné d'une analyse d'impact relative à la protection des données** afin qu'un débat parlementaire éclairé et effectif puisse avoir lieu à son sujet. C'est notamment une telle analyse qui permettra de séparer clairement la mission originelle de l'intégrateur de services fédéral de ses nouvelles missions, et d'évaluer la portée de l'extension des utilisateurs de l'intégrateur de services, et de mettre en évidence les adaptations nécessaires au dispositif actuel de la loi de 2012 (rédigée à une époque où le RGPD n'existait pas et où le rôle de l'intégrateur de services était plus limité). Une telle analyse devrait également permettre d'évaluer les critères et la méthode retenus pour identifier les sources authentiques de données, dans un contexte élargi d'offre des services de l'intégrateur de services fédéral, également aux entités fédérées et aux autorités publiques qui en dépendent (y compris la réflexion au sujet d'un accord de coopération national à ce sujet, couvrant le recours aux sources authentiques fédérales et fédérées et la garantie d'assurer la cohérence en la matière).

11. Enfin, dès lors que la **réforme du Règlement eIDAS** n'est pas votée à l'heure de la rédaction du Projet[5], l'Autorité est d'avis qu'en ce qu'il anticipe l'exécution de ce Règlement réformé, le Projet ne peut se trouver à un stade de rédaction final[6], et **la consultation de l'Autorité sur ce volet du Projet est prématurée**. Autrement dit, l'Autorité **réserve son analyse quant à l'exécution du Règlement eIDAS réformé et se limitera à émettre les commentaires nécessaires au regard des autres aspects de la modification de la loi de 2012**.

## II.2. Sources authentiques de données et autres sources de données

### II.2.1. Définitions

12. En droit positif le concept de « *source authentique* » est défini indirectement via la définition – liée – du concept de « *de donnée authentique* ». Le concept de « *source authentique* » consacré dans l'article 2, 6°, de la loi de 2012 est modifié par l'article 2 du Projet. Le concept de « *donnée*

[4] Voir le considérant n° 8.

[5] A la demande de l'Autorité, le demandeur a communiqué la dernière version du texte dont il disposait, soit un document de 211 pages en anglais (sans équivalence donc, des concepts en français ou en néerlandais) comprenant des modifications indiquées en suivi des modifications et dont la référence est PE-CONS 68/23 – 2021/0136 (COD).

[6] Voir d'ailleurs la note de bas de page n° 3.

*authentique* », consacré dans l'article 2, 5°, de la même loi, demeure quant à lui inchangé[7]. Désormais, plutôt qu'une « *banque de données dans laquelle sont conservées des données authentiques* », la source authentique devient « *un registre ou un système, sous la responsabilité d'un organisme de droit public ou d'une entité privée, qui contient des attributs relatifs à une personne physique ou morale et qui est considéré comme la source principale de ces informations ou est reconnu comme authentique en vertu du droit de l'Union ou du droit national, y compris la pratique administrative* » (souligné par l'Autorité).

13. L'exposé des motifs se limite à préciser que la « *définition de la source authentique a été alignée sur la définition contenue dans les propositions de modification du règlement eIDAS* », tandis que **la nouvelle approche introduite par le Projet introduit un réel flou quant à la portée du concept de source authentique de données**.

14. Dans ce contexte, l'Autorité a invité le demandeur à lui préciser l'objectif et la portée de la modification de la définition du concept de source authentique de données (recours au concept d' « *attribut* », abandon de la référence aux « *données authentiques* », *quid* de la référence à la « *pratique administrative* », etc.), et à lui communiquer les modifications en cours du Règlement eIDAS sur lequel il se base. Le demandeur a répondu dans un premier temps ce qui suit :

> « *La définition de source authentique dans le projet de loi a été* ***alignée sur la définition contenue (à l'époque) dans les propositions de modification du règlement eIDAS****. Dans la dernière version du projet de modification du règlement eIDAS (cfr. annexe, qui sera* ***soumis au vote au Parlement européen en février 2024. Le vote au Conseil suivra par la suite****.) la definition suivante est reprise: 'authentic source' means a repository or system, held under the responsibility of a public sector body or private entity, that contains and provides attributes about a natural or legal person or object and that is considered to be a primary source of that information or recognised as authentic in accordance with Union or national law, including administrative practice »*
> ***Nous devrons bien sûr nous aligner sur la toute dernière définition****.*
>
> *Dans la dernière version du projet de modification du règlement eIDAS, « attribute » est définie comme suit : « "attribute" means a characteristic, quality, right or permission of a natural or legal person or of an object; »*

[7] Soit une « *donnée récoltée et gérée par une instance dans une base de données et qui fait foi comme donnée unique et originale concernant la personne ou le fait de droit concerné, de sorte que d'autres instances ne doivent plus collecter cette même donnée* ».

***Une source peut contenir à la fois des données authentiques et des données non authentiques. C'est pourquoi il est essentiel de conserver la définition et la notion de données authentiques dans l'article 27****.*

***En réponse à la remarque du Conseil d'État selon laquelle il serait cohérent de maintenir le lien entre les définitions « source authentique » en « données authentiques » on a proposé d'améliorer la définition de source authentique comme suite****:*
*« un registre ou un système, sous la responsabilité d'un organisme de droit public ou d'une entité privée, qui contient des attributs relatifs à une personne physique ou morale et qui est considéré comme la source principale de ces données authentiques ou est reconnu comme authentique en vertu du droit national* » (mis en gras par l'Autorité).

Réinterrogé au sujet du concept de source authentique, le demandeur a dans un deuxièmement temps, précisé ce qui suit :

« *We stellen voor om naar aanleiding van jullie vragen en de vragen van de Raad van State* ***de definities te laten zoals ze bestaan in de huidige wet****.* ***Deze definities zijn geenszins in tegenspraak met de definities in de eIDAS verordening****. Ze wijzigen levert andere problemen op in de wet omdat de link met authentieke gegevens moet blijven bestaan. Niet elke bron bevat enkel authentieke gegevens, soms zijn er in één bron authentieke en niet authentieke gegevens. Daarom voorziet het gewijzigde artikel 27 het kwalificeren van de gegevens en niet automatisch van de gehele bron* » (mis en gras par l'Autorité).

15. **L'Autorité prend acte du fait que le demandeur renonce à modifier le concept de source authentique tel qu'il existe actuellement dans la loi de 2012**. Elle émet en outre les commentaires suivants.

16. **Premièrement**, l'Autorité est d'avis que **le Projet doit garantir que le dispositif de loi de 2012 distingue clairement l'échange de données issues de sources authentiques de données de l'échange de données qui *ne* sont *pas* issues de sources authentiques de données**. A cet égard, la logique selon laquelle des autorités publiques **doivent** recourir à la source de données disponible via l'intégrateur de services fédéral est justifiée sur le plan des principes de finalité et de qualité des données, lorsque cette source de données est authentique. **C'est en raison du caractère authentique de données qu'il est pertinent, sur le plan de ces principes, d'imposer aux**

**autres autorités publiques de recourir à la source de données concernée**[8]. C'est une logique qui ne transparaît pas des dispositions de la loi de 2012[9] de telle sorte qu'*in fine*, les réutilisations de données entre autorités peuvent être organisées sans qu'il soit juridiquement recouru à des sources authentiques de données. Ces considérations sont également à lier directement à la question de la portée des obligations d'un utilisateur (service public participant) ayant recours aux services de l'intégrateur de services fédéral[10].

17. Deuxièmement, **si *in fine*, dans le cadre du processus normatif, il était néanmoins décidé de modifier le concept de source authentique de données** en raison de la réforme du Règlement eIDAS, l'Autorité attire l'attention du demandeur sur les deux points suivants, relatifs au Projet tel qu'il est actuellement formulé.

18. Tout d'abord, **l'exposé des motifs devrait justifier la raison pour laquelle le concept de droit belge fédéral de source authentique de données devrait être complètement aligné sur le** concept qui sera consacré dans la réforme du **Règlement eIDAS**. Cette analyse devrait être reprise dans **l'analyse d'impact** relative à la protection des données qu'il conviendrait de réaliser compte-tenu de la portée du Projet.

19. Il s'agirait ainsi de déterminer si la (les) finalité(s) (les fonctions) du concept de source authentique du Règlement eIDAS sont identiques aux finalités (fonctions) du concept en droit belge et que partant, un concept propre au droit belge n'aurait plus d'utilité. **Dans ce cas, il conviendrait alors de se référer explicitement à la définition consacrée dans le Règlement eIDAS**.

20. A l'inverse, si le concept européen ne pouvait suffire à accomplir les objectifs du droit belge, le dispositif du Projet devrait alors comporter deux définitions, selon les finalités pertinentes poursuivies par la loi de 2012 et celles poursuivies par le Règlement eIDAS, de telle sorte que la portée des différents concepts ressorte clairement du Projet.

---

[8] Voir également le considérant n° 48 de l'avis n° 154/2023 de l'Autorité, rédigé comme suit (références omises, mise en gras et soulignement dans le texte original) :

« *L'Autorité est d'avis que sur le plan des principes, **ces dispositions renversent le paradigme juridique actuellement applicable aux traitements de données à caractère personnel en droit belge, conformément aux principes de légalité et de prévisibilité** consacrés dans les articles 8 CEDH et 22 de la Constitution. Ce faisant, **le Projet transpose la logique du traitement de données issues de sources authentiques de données à tout échange de données auquel est partie une autorité publique bruxelloise**[…], à charge pour celles-ci de conclure un protocole d'accord à cette fin*[…]. *Alors qu'en principe et en toutes hypothèses, un traitement de données à caractère personnel ne peut avoir lieu **que lorsqu'il est fondé juridiquement dans le cadre d'une compétence ou d'une obligation attribuée à une autorité publique** (presque toujours dans le cadre des traitements de données réalisés par les Autorités publiques, le traitement de données a lieu dans les cas visés à l'article 6, 1., c) et d)) et que ses **éléments essentiels sont déterminés par une norme du rang de loi**. étant entendu que selon les traitements de données concernés, l'encadrement par une norme du rang de loi sera **plus ou moins étendu**[…]. Autrement dit, il ne suffit pas pour qu'un traitement de données soit réalisable, qu'aucune disposition particulière ne s'y oppose* ».

[9] Voir l'article 4 de la loi de 2012, qui vise largement l'accès intégré « *aux données* ». L'article 8 de la loi de 2012, et en particulier son paragraphe 3, s'applique également que les données disponibles via l'intégrateur de service soient ou pas issues d'une source authentique de données.

[10] Voir les considérants nos 69 et s.

21. **C'est au demandeur qu'il appartiendrait de motiver cette analyse et ce, sur la base des dispositions finales et définitives du Règlement eIDAS réformé**. Sur ce point, l'Autorité attire également l'attention du demandeur sur le fait qu'une source authentique pourrait également et par exemple, comporter des attributs relatifs à des biens (à probablement reprendre dans le concept d'« *objects* » selon la réforme du Règlement eIDAS). La définition actuelle du Projet ne vise que les attributs relatifs à des personnes physiques ou morales[11].

22. Ensuite, l'Autorité souligne en outre que conformément aux principes de prévisibilité et de légalité consacré dans les articles 8 CEDH, 22 de la Constitution, 8 de la Charte européenne des droits fondamentaux et 6, 3., du RGPD, **« *la pratique administrative* » ne peut suffire à permettre la consécration comme authentique dans le cadre du Projet, d'une source de données** et ce, compte-tenu des conséquences juridiques y liées, sur le plan du traitement des données à caractère personnel. **L'Autorité a rappelé aux considérants nos 4-6[12] et 35-37[13] de son avis n°**

[11] Mais le demandeur a bien confirmé qu'il devrait s'aligner sur la dernière version du concept européen.

[12] En omettant les références, ces considérants sont rédigés comme suit (mise en gras et soulignement dans le texte original) :

« ***L'Autorité s'est déjà prononcée*** *en détails aux* ***considérants nos 5-19 de son avis précédent*** ***quant à l'application des principes de prévisibilité et de légalité consacrés dans les articles 8 CEDH et 22 de la Constitution*** *dans le contexte de l'accord de coopération partage de données et de la réutilisation des données issues de sources authentiques, et ce compte-tenu des spécificités du domaine couvert par cet accord et du dispositif prévu. L'Autorité* ***renvoie à ces considérations à titre préliminaire****.*

*En particulier au considérant n° 7 de son avis précédent, l'Autorité relève que les principes de prévisibilité et de légalité* « doivent être appliqués en prenant en compte la nature générale et abstraite du projet qui en substance, fixe un cadre pour l'échange en Wallonie entre autorités publiques de données à partir de sources authentiques de données en permettant une collecte unique auprès des citoyens et des entreprises, et pour le contrôle des traitements de données réalisés par ces autorités, sans prévoir directement des traitements de données particuliers (à quelques nuances près toutefois, voir […]). Ainsi, au-delà de cette finalité générale, le projet ne fixe pas lui-même les finalités déterminées et explicites des traitements des données provenant des sources authentiques, celles-ci ressortant d'autres textes le cas échéant futurs. […] ».

*Autrement dit concrètement,* ***la conformité des traitements de données mis en œuvre en exécution du Projet au regard des principes de prévisibilité et de légalité, devra être évaluée in concreto et systématiquement à l'aune de trois cadres normatifs*** *: celui régissant la source authentique de données ; celui du Projet ; et celui régissant l'activité du service public participant qui envisage de traiter la donnée issue de la source authentique concernée. Notamment, l'article 7, § 2, al. 2, du Projet s'inscrit dans cette logique lorsqu'il rappelle que* « Le recours aux services de la BCED[…] ne confère pas aux services publics participants le droit d'accéder à des données auxquelles ils n'auraient pas accès en consultant directement les sources de données authentiques ».

[13] En omettant les références, ces considérants sont rédigés comme suit (mis en gras et soulignement dans le texte original) :

« *L'Autorité relève que l'échange de données à caractère personnel nécessite bien toujours un cadre normatif conforme aux principes de prévisibilité et de légalité rappelés précédemment. Tout le Projet est d'ailleurs tourné vers l'encadrement (certes, mais à la fois logiquement, partiel, comme cela a été rappelé) des échanges de données issues de sources authentiques. Que des échanges de données puissent déjà exister entre autorités publiques en l'absence d'une labellisation d'une banque de données comme étant une source authentique de données est indifférent dans l'analyse.*

***L'Autorité est d'avis que le Projet doit à tout le moins prévoir qu'un arrêté du Gouvernement doit être adopté pour qualifier une banque de donnée de source authentique de données****. En effet, la qualité de source authentique qui est attribuée à une banque de données constitue clairement un élément essentiel des traitements de données mis en place (elle relève de la finalité du traitement) : c'est de cette qualité que découle le mode indirect (et obligatoire) de collecte des données auprès de la source concernée, via la BCED, en exécution du Projet. Ce n'est par conséquent que compte-tenu des spécificités du Projet et de sa logique (à savoir la mise en place d'un dispositif général organisant le recours systématique aux sources authentiques de données) que l'Autorité a accepté antérieurement que le statut de source authentique puisse être attribué par une norme réglementaire (et non directement par une norme du rang de loi), sans pour autant méconnaître les principes de prévisibilité et de légalité consacrés dans les articles 8 CEDH et 22 de la Constitution[…]. Déléguer ce pouvoir à une autorité publique telle que la BCED (in concreto, à son responsable) méconnaît ces principes.*

*S'agissant des conditions auxquelles doit répondre une base de données pour pouvoir être désignée comme source authentique de donnée, l'article 5, § 1er, 3°, du Projet prévoit que* « la banque de données trouve son fondement dans une norme de valeur

**143/2023 l'applicabilité des principes de prévisibilité et de légalité à l'échange de données issues de sources authentiques et renvoie à ces développements**.

### II.2.2. Désignation et critères de désignation des sources authentiques

23. Dans la même veine que le commentaire précédent, **le Projet modifie le principe actuellement consacré dans l'article 27, § 2, de la loi de 2012, selon lequel** sur proposition du Comité de coordination[14], **c'est le Roi qui détermine, par arrêté délibéré en Conseil des ministres**, d'une part, les critères sur la base desquels des données sont qualifiées d'authentiques (critères qui sont désormais directement repris par le Projet, dans le dispositif de la loi de 2012), et d'autre part, **quelles données peuvent être qualifiées d'authentiques**. Le Projet prévoit désormais ce qui suit :

> « *Le comité de coordination qualifie les données d'authentiques si elles répondent aux critères suivants :*
>
> *1. l'enregistrement des données et leur communication résultent de missions assignées par ou en vertu d'une loi, d'un décret ou d'une ordonnance ;*
>
> *2. l'utilisateur visé à l'article 2, 10°, a) à g), qui est chargé de collecter ou de gérer les données, prévoit et respecte des procédures garantissant que les données sont en permanence exactes, complètes, sûres, lisibles et disponibles, et en informe périodiquement le comité de coordination* ».

24. Le commentaire du premier critère est rédigé comme suit :

> « *Un premier critère pour qualifier une donnée de donnée authentique réside dans le fait que l'enregistrement de cette donnée doit être prescrit par ou en vertu d'une loi, d'un décret ou d'une ordonnance. Ce premier critère est particulièrement important pour les données collectées par des organismes extérieurs au secteur public. En effet, ces organismes - par exemple, les fédérations de praticiens de certaines professions libérales - collectent également des données dont l'enregistrement n'est pas imposé par une disposition légale ou réglementaire. De telles données, sur lesquelles les autorités publiques ne peuvent exercer aucun contrôle, ne peuvent jamais être qualifiées de données authentiques. En effet, une fois qualifiées comme telles, les autorités publiques seront pratiquement obligées de travailler avec*

légale » (souligné par l'Autorité). *L'Autorité est d'avis que l'expression « de valeur légale » est ambigüe et doit être remplacée par « décret ». Compte-tenu des principes de prévisibilité et de légalité juste rappelés,* ***il est nécessaire que les éléments essentiels des traitements de données réalisés par l'intermédiaire d'une banque de données constituant une source authentique de données soient définis dans une norme du rang de loi****[...]. Ne peuvent à cet égard être identifiée comme source authentique que les banques de données dont les éléments essentiels sont déterminés par une norme du rang de loi.* ***S'agissant des ordres juridiques wallon et de la Communauté française, il convient par conséquent de se référer au décret****. L'article 5, § 1er, 3°, du Projet doit par conséquent être adapté en conséquence* ».

[14] Le Comité de coordination se compose, selon le Projet, du dirigeant de chaque utilisateur visé à l'article 2, 10°, a) à g), du dirigeant de chaque intégrateur de services, au sens de l'article 2, 1°, et du président du Comité de direction du Service public fédéral Stratégie et Appui.

> *ces données comme si elles les avaient collectées elles-mêmes. Les données enregistrées et gérées par des organismes extérieurs au secteur public peuvent donc être qualifiées de données authentiques, à condition qu'il s'agisse également de données dont l'enregistrement découle d'une exigence légale ou réglementaire.*
>
> *Ce critère ne signifie pas que les données doivent être expressément énumérées dans une loi, un arrêté royal, un décret ou une ordonnance, mais plutôt que l'enregistrement des données doit résulter des missions imposées par ou en vertu de la loi de l'organisme qui les enregistre* » (souligné par l'Autorité).

25. L'Autorité a interrogé le demandeur sur la raison de la suppression du rôle du Roi (via un arrêté délibéré en Conseil des ministres). Celui-ci a répondu ce qui suit :

> « *Il nous semble opportun d'inclure explicitement les conditions dans la loi afin d'offrir une plus grande sécurité juridique aux organismes concernés.* ***Le comité de coordination est certainement le mieux placé pour décider de cette question, car il dispose de l'expertise nécessaire****. À cet égard, il convient de se référer à son manuel relative à la mise en place d'une source authentique.*
> *(Cfr. https://bosa.belgium.be/sites/default/files/documents/bosa_dt_guide_pratique_-_mise_en_place_dune_source_authentique_v1.0.pdf, publié la page web suivante : https://bosa.belgium.be/fr/themes/administration-numerique/composants-et-plateformes-numeriques/sources-authentiques)*
> *Ce comité fournit également des conseils aux organismes concernés pour se conformer aux conditions. À notre avis,* ***il n'y a pas de valeur ajoutée à faire valider cela par un arrêté royal*** » (mis en gras par l'Autorité).

26. Avant tout, **l'Autorité est d'avis que l'identification des critères permettant la désignation d'une source authentique dans la loi de 2012 elle-même constitue un apport positif du Projet sur le plan de la protection des données** à caractère personnel. De cette manière, le Projet assure qu'un débat parlementaire pourra avoir lieu sur le sujet et garantit une meilleure stabilité juridique au sujet.

27. Cela étant précisé, l'Autorité renvoie aux **considérants nos 4-6 et 35-36 de son avis n° 143/2023**[15]. **La nécessité d'un arrêté royal (en l'occurrence, délibéré en Conseil des ministres) afin d'identifier les données (ou sources) authentiques se justifie au regard des principes de prévisibilité et de légalité** : un tel arrêté constitue un **acte normatif** qui peut en

[15] Voir les notes de bas de page nos 12-13.

l'occurrence, compte-tenu de la pratique d'avis antérieure de l'Autorité, participer à la détermination des éléments essentiels des traitements de données concernés en désignant les sources (ou données) authentiques concernées[16]. Une qualification par le Comité de coordination ne constitue pas une norme et ne peut satisfaire aux exigences de prévisibilité et de légalité. **L'Autorité est d'avis que le Projet doit être adapté sur ce point**.

28. En outre et comme l'Autorité l'a souligné dans sa pratique d'avis juste rappelée[17], **en relation avec le premier critère de désignation d'une source authentique en vertu du Projet (mission légale)**, l'application des principes de prévisibilité et de légalité requiert que **la mission (ou l'obligation) de l'autorité publique (ou de l'entité privée)** en vertu de laquelle la donnée authentique concernée doit être collectée ou crée[18], **doit être consacrée dans une norme du rang de loi, tout comme les éléments essentiels du traitement de cette donnée par l'autorité publique concernée**. L'Autorité considère par conséquent que le Projet (dispositif et exposé des motifs) **doit être adapté** sur ce point et qu'il n'est pas justifié de supprimer la nécessité d'un arrêté royal délibéré en Conseil des ministres tel qu'actuellement prévue par la loi de 2012.

29. Ensuite, **quant aux critères de désignation d'une source authentique de données**, l'Autorité s'est déjà prononcée au considérant n° 64 de son avis n° 154/2023 et aux considérants nos 38-39 de son avis n° 143/2023. Le premier critère prévu par le Projet prévoit que « *l'enregistrement et la communication des données* » doit résulter des missions légales concernées.

30. A ce sujet, plus que « *l'enregistrement* », l'Autorité attire l'attention du demandeur sur le fait que c'est en principe et plutôt **la collecte ou la création de la donnée** qui doivent résulter d'une mission (légale) de la source concernée. Ainsi, **l'élément décisif est que compte-tenu de ses missions légales en relation avec la donnée concernée, et en particulier, sa collecte/création et mise à jour, l'entité concernée est la mieux placée pour en garantir la qualité et la communication[19] à d'autres entités pour les finalités qu'elles poursuivent**.

31. Certes, il n'est **en effet pour autant pas exclu que l'enregistrement de la donnée puisse** dans certaines hypothèses, **être déterminant**, lorsque compte-tenu de la finalité des traitements prévus

[16] Ainsi, l'Autorité a accepté par le passé que la simple désignation de la source authentique puisse se faire par une mesure réglementaire (un arrêté du Gouvernement wallon dans l'avis en question), pour autant que le reste des éléments essentiels des traitements envisagés soient consacrés dans une norme du rang de loi.

[17] En particulier et déjà au considérant n° 19 de son avis n° 65/2019 du 27 février 2019 *concernant un projet d'accord de coopération modifiant l'accord de coopération du 23 mai 2013 entre la Région wallonne et la Communauté française portant sur le développement d'une initiative commune en matière de partage de données et sur la gestion conjointe de cette initiative (CO-A-2019-014 + CO-A-2019-044)*, l'Autorité rappelait que la source authentique de données doit être créée et organisée, *mutatis mutandis*, par une norme du rang de loi.

[18] Voir le considérant n° 22.

[19] Sur ce point l'Autorité accueille favorablement que le Projet vise également la communication de la donnée dans son premier critère.

par la loi, un besoin spécifique et justifié de conservation centralisée (d'intégration de données en vue de la création d'une source authentique) est nécessaire, comme l'illustre l'hypothèse du Registre national[20]. L'Autorité est d'avis que sur ce point, **le demandeur devrait préciser le dispositif du Projet**.

32. S'agissant du deuxième critère, «*l'utilisateur visé à l'article 2, 10°, a) à g), qui est chargé de collecter ou de gérer les données, prévoit et respecte des procédures garantissant que les données sont en permanence exactes, complètes, sûres, lisibles et disponibles, et en informe périodiquement le comité de coordination* ». L'Autorité est d'avis **qu'il convient également de se référer au cadre normatif applicable à l'utilisateur concerné**. En effet, **et compte-tenu des finalités poursuivies, ce cadre normatif devrait consacrer des dispositions relatives à la qualité des données, à leur mise à jour** (identification des événements entraînant une mise à jour/modification des données, d'une éventuelle fréquence, etc.), etc.

**II.3. Services publics participants et utilisateurs**

33. Le concept de « *service public participant* » consacré dans l'article 2, 10°, de la loi de 2012 est remplacé par celui d' « *utilisateur* ». L'exposé des motifs explique ce qui suit à ce sujet :

> « *Le terme « service public participant » a été remplacé par le terme « utilisateur » car les services publics ne sont pas les seuls à pouvoir mettre à disposition des données par l'intermédiaire de l'intégrateur de services fédéral. Conformément à l'article 46 de la loi, d'autres organismes peuvent également être désignés. En outre, les destinataires des données seront à la fois les services publics et d'autres titulaires de droits tels que les citoyens et les entreprises et leurs représentants.*
>
> *Le terme « utilisateur » a été défini plus clairement et il a été ajouté que les données mises à disposition par l'intégrateur de services fédéral le sont pour tous les titulaires de droits sur ces données. Il peut s'agir des ayants droit d'une source authentique désignés dans la législation sur la source et à qui les données doivent être communiquées. Il peut s'agir de la personne concernée qui a le droit de savoir quelles données la concernant sont traitées. Il peut s'agir du détenteur d'un portefeuille européen d'identité numérique qui peut y recevoir des données des autorités publiques pour les proposer à des tiers. Il peut s'agir de ceux qui ont droit à des informations en vue de leur réutilisation, des organisations qui auront droit à des données publiques, en Belgique et à l'étranger, selon la DGA.*

[20] Voir la loi du 8 août 1983 *organisant un registre national des personnes physiques* (et son article 4, par exemple).

*Le Comité permanent de contrôle des services de police, le Comité permanent de contrôle des services de renseignements, l'Organe de coordination pour l'analyse de la menace sont ajoutés comme utilisateur. Ils doivent pouvoir utiliser les données mises à disposition pour l'exécution de leurs tâches.*

*Le comité de sécurité de l'information a été ajouté. Ce comité est compétent en matière de communication de données personnelles* » (souligné par l'Autorité).

34. Le Projet ajoute plusieurs instances au concept d'utilisateur, parmi lesquelles :

- Le Comité permanent de contrôle des services de police ;
- Le Comité permanent de contrôle des services de renseignements ;
- L'Organe de coordination pour l'analyse de la menace ;
- Le Comité de sécurité de l'information ;
- La police intégrée, les services appartenant à la Défense (le Ministère de la Défense est déjà visé par la loi de 2012) ;
- Le pouvoir judiciaire y compris les services d'assistance à ses membres, les personnes morales de droit public visées à l'article 1er, 3°, de la loi du 22 juillet 1993 *portant certaines mesures en matière de fonction publique*[21] ;

[21] Soit :
« *- la Régie des bâtiments;*
*- l'Agence fédérale pour la Sécurité de la chaîne alimentaire;*
*- le Bureau d'intervention et de restitution belge;*
*- (...); <L 2003-04-03/68, art. 33, 016;* ***En vigueur :*** *01-12-2006>*
*- l'Office central d'Action sociale et culturelle du Ministère de la Défense;*
*- l'Institut géographique national;*
*- [2 le War Heritage Institute]2;*
*- l'Office de contrôle des mutualités et des unions nationales de mutualités;*
*- l'Office de contrôle des assurances;*
*- [1 ...]1;*
*- le Fonds des accidents du travail;*
*- le Fonds des maladies professionnelles;*
*- [2 ...]2;*
*- la Caisse auxiliaire d'assurance maladie-invalidité;*
*- la Caisse auxiliaire de paiement des allocations de chômage;*
*- [1 ...]1;*
*- l'Office national d'allocations familiales pour travailleurs salariés;*
*- l'Office national de sécurité sociale;*

- Les personnes physiques ou morales auxquelles des missions de service public ou d'intérêt général sont conférées par la loi et qui ne relèvent pas de la loi du 21 mars 1991 *portant réforme de certaines entreprises publiques économiques* ;

- Toute personne et autorité désignée par le Roi en exécution de l'article 46[22], dans la mesure où elle met à disposition une ou plusieurs sources authentiques ou bases de données ou récupère des données par le biais de l'intégrateur de services fédéral ;

- Et toute personne et autorité qui, selon la réglementation fédérale ou européenne et selon les conditions attachées aux données des sources authentiques ou des sources de données des utilisateurs visés à l'article 2, 10°, a à g, est habilitée à consulter ou à recevoir ces données.

35. Tel que modifié, l'article 2, 10°, de la loi de 2012 comporte par ailleurs toujours une exception visant l'intégrateur de services fédéral lui-même ainsi qu'une série d'institutions liées à la sécurité sociale. Sur ce point, par souci de cohérence, l'Autorité invite le demandeur à **modifier sa référence à l'article 1er, 3°, de la loi du 22 juillet 1993 *portant certaines mesures en matière de fonction publique* en tenant compte de cette exception**.

36. Dans ces conditions, **au-delà des quelques précisions de l'exposé des motifs[23], il n'est plus possible d'identifier concrètement qui deviennent les utilisateurs potentiels au sens de la**

---

*- [4 ...]4;*

*- l'Institut national d'assurances sociales pour travailleurs indépendants;*

*- l'Institut national d'assurance maladie-invalidité;*

*- l'Office national des vacances annuelles;*

*- l'Office national de l'emploi;*

*- [5 le Service fédéral des Pensions;]5*

*- la Banque-Carrefour de la sécurité sociale;*

*- (le Bureau fédéral du Plan;) <L 2004-12-27/30, art. 506, 017; **En vigueur :** 10-01-2005>*

*(- l'Institut pour l'égalité des femmes et des hommes;) <L 2003-02-27/50, art. 2, 015; **En vigueur :** 03-04-2003>*

*- [5 ...]5;*

*(- Agence des appels aux services de secours;) <L 2006-07-20/39, art. 75, 019; **En vigueur :** 07-08-2006>*

*(- Agence fédérale des médicaments et des produits de santé;) <L 2006-07-20/78, art. 16, 020; **En vigueur :** 01-01-2007>*

*[2 - la plate-forme eHealth;]2* ».

[22] L'article 46 de la loi de 2012 s'énonce comme suit :

« *Sous les conditions et selon les modalités qu'Il détermine, le Roi peut, par arrêté délibéré en Conseil des Ministres sur proposition du comité de concertation des intégrateurs de services et après avis de la Commission de la protection de la vie privée, étendre l'ensemble ou une partie des droits et obligations découlant de la présente loi et de ses mesures d'exécution à des personnes ou instances autres que les services publics participants. Une telle extension des droits et obligations ne peut pas porter sur des tâches relevant du domaine de fonctionnement d'un autre intégrateur de services* ».

[23] La seule précision concrète concerne le fait que des utilisateurs sont des titulaires de droits sur les données concernées :

« *Le terme « utilisateur » a été défini plus clairement et il a été ajouté que les données mises à disposition par l'intégrateur de services fédéral le sont pour tous les titulaires de droits sur ces données. Il peut s'agir des ayants droit d'une source authentique désignés dans la législation sur la source et à qui les données doivent être communiquées. Il peut s'agir de la personne concernée qui a le droit de savoir quelles données la concernant sont traitées. Il peut s'agir du détenteur d'un portefeuille européen d'identité numérique qui peut y recevoir des données des autorités publiques pour les proposer à des tiers. Il peut*

**loi de 2012**. L'Autorité a interrogé le demandeur quant à la motivation et les raisons pratiques qui ont conduit à une telle extension du concept de « service public participant », au-delà de ce qui est précisé dans l'exposé des motifs. Elle l'a également invité à illustrer quelles pouvaient être les autres personnes visées par l'article 46 de la loi de 2012 ainsi que quelles étaient les personnes privées susceptibles de mettre à disposition des sources authentiques. L'Autorité n'était plus sûre non plus de percevoir quel demeurait l'intérêt de l'article 46 de la loi de 2012. Elle a interrogé le demandeur à ces sujets, et celui-ci précise ce qui suit :

> « *L'extension des utilisateurs concerne en effet les personnes et les entités qui peuvent consulter ou recevoir des données par l'intermédiaire de l'intégrateur de services fédéral.*
> *Il reste important de prévoir la possibilité sur base de l'article 46* ***d'élargir la catégorie d'entités pouvant fournir des données via l'intégrateur de services fédéral (par exemple, la fédération des notaires, la Chambre nationale des huissiers de justice, l'Ordre des avocats, l'ITAA - Institut des conseillers fiscaux et comptables,*** *…).*
>
> *À titre d'exemple de raison* ***d'élargir la catégorie des destinataires****, on peut mentionner le FOD Mobilité, qui peut, conformément à sa propre législation,* ***communiquer des données à des entités privées*** *(i.e. autres que les services publics participants), ce qui n'est pas prévu dans les dispositions actuelles de la loi de 2012.*
>
> *La modification de la catégorie des utilisateurs vise à étendre les* ***catégories potentielles de destinataires*** *auxquels les données sont accessibles. Alors que* ***précédemment, l'accès ne concernait que la communication entre les services publics participants****, l'extension concerne la communication des utilisateurs concernés à toutes les parties autorisées à recevoir ces données de ces utilisateurs. Ceci est* ***nécessaire pour répondre à diverses obligations et besoins dans le cadre de l'application de la Digital Governance Act, de la Single Digital Gateway, de eIDAS*** *modifié (la portefeuille numérique), pour lesquels l'intégrateur de services fédéral interviendra désormais pour la mise à disposition de données aux ayants droit (personnes et entités)* » (mis en gras par l'Autorité).

Dans un deuxième temps, au sujet de ces diverses obligations, le demandeur a apporté les précisions suivantes :

> « *Single digital gateway*
> - *Verordening (EU) 2018/1724 van het Europees Parlement en de Raad van 2 oktober 2018 tot oprichting van één digitale toegangspoort voor informatie, procedures en diensten*

*s'agir de ceux qui ont droit à des informations en vue de leur réutilisation, des organisations qui auront droit à des données publiques, en Belgique et à l'étranger, selon la DGA* » (souligné par l'Autorité).

*voor ondersteuning en probleemoplossing en houdende wijziging van Verordening (EU) nr. 1024/2012, art. 6 en art. 14*

- *UITVOERINGSVERORDENING (EU) 2022/1463 VAN DE COMMISSIE van 5 augustus 2022 tot vaststelling van technische en operationele specificaties van het technisch systeem voor de grensoverschrijdende geautomatiseerde uitwisseling van bewijs en de toepassing van het eenmaligheidsbeginsel overeenkomstig Verordening (EU) 2018/1724 van het Europees Parlement en de Raad, art. 1 tot en met 36*
- *SPF BOSA est responsable pour le développement et de mettre à disposition le Only Once Technical System en Belgique, en collaboration avec data providers en Belgique, les autres . L'attribution de cette mission est prévue dans (le projet de) l'accord de coopération entre le gouvernement fédéral et les entités fédérées.*

*Data governance act*

- *het vervullen van de rollen van centraal informatiepunt en van bevoegd orgaan voor de technische bijstand zoals bedoeld respectievelijk in de artikelen 8 en 7, 1° van de Europese Verordening (EU) 2022/868 van het Europees Parlement en de Raad van 30 mei 2022 betreffende Europese datagovernance en tot wijziging van Verordening (EU) 2018/1724*

*eIDAS act (wijziging)*

- *in het ontwerp van wijziging van eIDAS Act wordt voorzien dat elke lidstaat een Europese portemonnee voor digitale identiteit moet aanbieden. In België zal FOD BOSA instaan voor de ontwikkeling en ter beschikking stelling van die Europese portemonnee voor digitale identiteit. Het ontwerp van wijziging van eIDAS werd nog niet goedgekeurd dus er kan in de wettekst nog niet naar verwezen worden.*

  *Conforme à la définition prévue dans le projet de modification de eIDAS Act, le portefeuille européen d'identité numérique est un moyen d'identification électronique qui permet à l'utilisateur de stocker, de gérer et de valider en toute sécurité des données d'identification personnelle et des attestations électroniques d'attributs afin de les fournir aux parties utilisatrices et aux autres utilisateurs des portefeuilles européens d'identité numérique, et de signer au moyen de signatures électroniques qualifiées ou d'apposer des cachets au moyen de cachets électroniques qualifiés* ».

37. L'Autorité prend acte de ces explications. Elle attire néanmoins l'attention du demandeur sur le fait que les **h) et g) de l'article 2, 10°,** de la loi de 2012 tel que modifiée par le Projet, **semblent se recouper pour partie**. En effet, le g), qui se réfère à l'article 46 du Projet, vise également toute personne et autorité désignée par le Roi qui « *récupère* » des données par le biais de l'intégrateur de services fédéral. Or le h) vise déjà très largement les destinataires des données disponibles via l'intégrateur.

38. **Plus largement, le f), très large, semblerait également pouvoir viser des entités citées par le demandeur afin d'illustrer la portée de l'article 46.** Ainsi, « *la fédération des notaires, la Chambre nationale des huissiers de justice, l'Ordre des avocats, l'ITAA - Institut des conseillers fiscaux et comptables* » ne sont-elles pas déjà des entités qui sont chargées par la législation en vigueur de certaines missions d'intérêt public ou à tout le moins, d'obligations légales spécifiques en relation avec les données qu'elles collecteraient et qui pourraient être pertinentes dans la mise en œuvre de la loi de 2012 ?

39. Par ailleurs, **l'article 46 de la loi de 2012 ne se limite pas à viser les entités qui « *fournissent* » des données via l'intégrateur de services fédéral**. Plus largement, et tel que modifié par le Projet, celui-ci donne en effet le pouvoir au « *d'étendre l'ensemble ou une partie des droits et obligations découlant* » de la loi de 2012 à des « *personnes ou instances autres que les utilisateurs visés à l'art. 2, 10°, a) à f), et h)* ».

40. Dans ces conditions, l'Autorité est d'avis que le demandeur doit **clarifier le dispositif du Projet et modifier les articles 2, 10, et 46 de la loi de 2012 de manière telle que ceux-ci reflètent correctement les intentions communiquées**, à savoir, pouvoir permettre, via l'article 46 du Projet, que des entités autres que les instances publiques visées actuellement par le Projet, puissent communiquer des données via l'intégrateur de services fédéral, lorsque celles-ci sont chargées d'une obligation légale ou d'une mission d'intérêt public imposant la collecte (ou la création) des données concernées. **Le Projet doit identifier et délimiter clairement les différentes entités concernées** : les destinataires des données (catégorie la plus large), les entités publiques (selon l'exposé des motifs, sont visés « les services publics ») et les entités privées chargées de missions d'intérêt public (ou obligations légales) spécifiques.

41. Par ailleurs, l'Autorité est d'avis que l'article 46 de la loi de 2012, y compris tel que modifié par le Projet, **est problématique au regard des principes de prévisibilité et de légalité rappelés précédemment**[24] en ce qu'il permet au Roi de moduler les droits et obligations prévus dans la loi de 2012 selon les instances à qui il étendrait l'application du dispositif en Projet. De nouveau, l'Autorité est d'avis qu'il **doit être reformulé au regard des intentions du demandeur (en limitant l'extension à la communication de données telle qu'évoquée précédemment)** et ce d'autant plus que désormais, la loi de 2012 telle que modifiée par le Projet voit sa portée étendue (l'intégrateur de services se voit attribuer de nouvelles missions par exemple) : **la loi de 2012 s'étend désormais au-delà de l'échange de données entre autorités publiques**.

[24] Voir le considérant n° 22.

42. En outre, l'Autorité rappelle que le principe du recours à l'intégrateur de services fédéral n'est en principe **pas contraignant**[25]. Dans cette logique, l'extension aux entités privées de l'application de la loi de 2012 **devrait par conséquent également être une faculté pour celles-ci**, comme pour les utilisateurs visés à l'article 2, 10°, a) à g), de la loi de 2012 telle que modifiée par le Projet. **A défaut**, la **différence de traitement devrait être justifiée** par le demandeur au regard du principe d'égalité, question au sujet de laquelle il appartient ensuite au Conseil d'Etat de se prononcer.

### II.3. Missions de l'intégrateur de services

#### II.3.1. Echange de données, attestation de données et portefeuilles d'identité

43. L'article 4, 1°, de la loi de 2012 tel que modifié par le Projet prévoit que l'intégrateur de services « *reçoit, conserve temporairement pendant le temps nécessaire pour la réalisation de la finalité poursuivie, et donne suite aux demandes de consultation et de communication des données enregistrées dans une ou plusieurs bases de données ou procède à leur communication intégrée et à l'attestation de ces données* » (souligné par l'Autorité). La conservation est également visée par l'article 4, 8°, en projet, de la loi de 2012.

44. Le Projet utilise des concepts qui n'existent pas encore en droit positif tels que ceux de « *portefeuilles d'identité numérique* » et d' « *attestations de données* ». Ainsi, tel que modifié par le Projet, l'article 4 de la loi de 2012 prévoit que l'intégrateur de services communique les données « *enregistrées dans une ou plusieurs bases de données ou procède à leur communication intégrée et à l'attestation de ces données* »[26]. L'article 12, § 1er, de la loi de 2012 tel que modifié par le Projet vise la force probante des attestations de données, et son paragraphe 2 vise une assimilation du document papier à l'attestation numérique.

45. L'intégrateur de services « *élabore les modalités techniques et les conditions visant à développer et connecter les canaux d'accès, y compris les services web, les applications mobiles, les portefeuilles d'identité numérique et les portails en ligne, de la manière la plus efficace et la plus sûre possible* »[27].

46. Au sujet de ces missions, l'exposé des motifs précise ce qui suit : « *L'attestation des données est ajoutée comme première mission mentionnée à l'article 4. À la lumière des projets actuels et futurs en application des propositions de modification du règlement eIDAS, tels que le développement du portefeuille d'identité numérique, il est également prévu que les citoyens puissent recevoir des attestations confirmant l'authenticité des informations publiques. À l'avenir, l'intégrateur de services*

[25] Voir les considérants nos 69 et s.

[26] Article 4, 1°, de la loi de 2012 telle que modifiée par le Projet.

[27] Article 4, 4°, de la loi de 2012 telle que modifiée par le Projet.

*fédéral devra donc également être en mesure de mettre à disposition ce type d'informations* » (souligné par l'Autorité).

47. L'Autorité a interrogé le demandeur quant à la portée la mission visée au considérant n° 45 (article 4, 4°, de la loi de 2012 tel que modifié par le Projet), en particulier au regard de la mission visée à l'article 4, 5°, de la loi de 2012 relative aux modalités techniques et conditions relatives à la communication entre les banques de données ou les sources authentiques et le réseau. **L'article 4, 4°,** de la loi vise-t-il bien l'accès aux banques de données et source authentiques de données ? Le demandeur a répondu ce qui suit « *En effet, comme mentionné dans cette article, il s'agit des « canaux d'accès » (aux banques de données)* ». Le 4° ne précise cependant pas qu'il est question de canaux d'accès « aux banques de données ».

48. L'Autorité est d'avis que les 4° et 5°, de l'article 4, de la loi de 2012 telle que modifiée par le Projet **doivent être clarifiés de manière telle que soient clairement distinguées les missions qui relèvent de l'échange de données issues de banques de données (sources authentiques ou pas) entre utilisateurs, et les autres missions qui concernent l'exécution de la future modification du Règlement eIDAS** (et au sujet desquelles l'Autorité ne se prononce pas).

49. Enfin, s'agissant de **l'intégration de données**, l'Autorité observe que le demandeur maintient dans l'article 4, 8°, de la loi de 2012, tel que modifié par le Projet, la possibilité de développer des applications aux fins de l'intégration de données. Sur ce point, l'Autorité attire le demandeur sur les réserves sérieuses qu'elle a émises, dans le domaine de l'échanges de données **issues de sources authentiques**, à propos du concept de banque de données issues de sources authentiques qui, *in concreto*, revient à intégrer des données issues de sources authentiques[28]. Sur le plan de la protection des données, l'intégration de services est à préférer à l'intégration de données. Bien qu'il soit clair que la disposition en projet ne puisse juridiquement suffire à elle-même pour fonder les traitements de données qu'elle vise (intégration de données, agrégation de données, enrichissement de données, etc.), l'Autorité rappelle néanmoins que conformément aux principes de prévisibilité et de légalité[29], de tels traitements de données à caractère personnel ne pourront être mis en œuvre que si le cadre normatif régissant les activités de l'utilisateur le permet, et ce, dans la mesure permise par ce cadre normatif.

### II.3.2. Mise à disposition d'applications réutilisables

50. L'article 4, 8°, de la loi de 2012 tel que modifié par le Projet prévoit que l'intégrateur de services développe « *développe des applications réutilisables utiles pour l'intégration, l'agrégation, la*

[28] Dernièrement, voir les considérants nos 65-71 de l'avis n° 154/2023.

[29] Voir les notes de bas de page nos 12-13.

*transformation, l'enrichissement, le filtrage, l'anonymisation, la pseudonymisation, la généralisation, la suppression, la randomisation, la conservation sécurisée, la mise à disposition et l'échange de données conservées dans les bases de données* » (souligné par l'Autorité).

51. Avant tout, comme le Conseil d'Etat[30], l'Autorité est d'avis que le dispositif du Projet lui-même, doit **définir les traitements de données qui sont envisagés**, à l'aune de l'exposé des motifs (intégration, agrégation, transformation, etc.).

52. Ensuite, l'exposé des motifs précise ce qui suit :

> « *La conservation concerne la conservation temporaire et est donc une disposition générique pour la mise en cache temporaire. Il ne s'agit donc en aucun cas d'une conservation permanente des données. Il s'agit uniquement du stockage technique temporaire pour pouvoir délivrer des attestations ou établir des certificats d'identification, par exemple. La conservation n'a lieu que si elle est nécessaire au traitement et la période de conservation temporaire est limitée dans le temps à un maximum de 5 jours et est déterminée en fonction du traitement demandé par l'utilisateur. La mise à disposition et l'échange de données parlent d'eux-mêmes.*
>
> *Les utilisateurs peuvent choisir, éventuellement à la demande d'une autorité compétente, de faire appel aux applications énumérées ci-dessus de l'intégrateur de services fédéral* » (souligné par l'Autorité).

53. Dans ce contexte, l'Autorité a interrogé le demandeur quant à la question de savoir s'il était bien exclusivement question du développement de logiciels (programmes) ou s'il était également question de prestation de services. Elle l'a également interrogé quant à la signification du caractère « *réutilisable* » des applications concernées.

54. Le demandeur a répondu ce qui suit :

> « *L'article 4, 8°, concerne expressément la mission de développement. La mise (éventuelle) de ces applications à disposition des utilisateurs est mentionnée à l'article 12, 12°.*
>
> *En utilisant le terme "Réutilisable", nous souhaitons clairement indiquer qu'il n'est pas prévu de développer la même application à partir de zéro pour chaque utilisateur* ».

[30] P. 5 de son avis précité.

55. Ceci ne permet pas d'identifier s'il est également question d'offre de services, le terme « mise à disposition » étant flou à ce sujet. **Il incombe au demandeur de clarifier le dispositif du Projet sur ce point** étant entendu que cela a un impact sur le plan du traitement de données à caractère personnel. Alors que l'offre d'une application sur la forme d'un service impliquera un traitement de données à caractère personnel, tel ne sera en principe pas le cas de la fourniture au demandeur d'une application (un programme informatique) qu'il doit installer sur son propre système d'information, paramétrer et faire fonctionner lui-même.

56. Interrogé une seconde fois au sujet de cette disposition et de sa relation avec l'article 4, 12°, de la loi de 2012 telle que modifiée par le Projet, le demandeur a notamment répondu ce qui suit :

> « *Voor alle duidelijkheid zal als volgt de terbeschikkingstelling van de ontwikkelde toepassingen uitdrukkelijk worden toegevoegd in 4.4° en 4.8°, en wordt de tekst van 4.12° als volgt aangepast:*
>
> *"4° het uitwerken van de technische modaliteiten om de toegangskanalen zo efficiënt en veilig mogelijk uit te bouwen; het uitwerken van de technische modaliteiten en de voorwaarden om de toegangskanalen, waaronder webdiensten, mobiele applicaties, de Europese portemonnee voor digitale identiteit en online portalen, zo efficiënt en veilig mogelijk uit te bouwen, met elkaar te verbinden en ter beschikking te stellen;"*
>
> *"8° het ontwikkelen en het ter beschikking stellen van herbruikbare toepassingen die nuttig zijn voor de integratie, de aggregatie, de transformatie, de verrijking, de filtering, de anonimisering, de pseudonimisering, de veralgemening, de schrapping, de randomisering, de beveiligde bewaring, terbeschikkingstelling en uitwisseling van in de gegevensbanken opgeslagen gegevens;"*
>
> *"12° het ontwikkelen, het testen, het onderhouden, het corrigeren en het ter beschikking stellen van de toepassingen en de systemen die nodig zijn om de voorgaande opdrachten te realiseren en de verwerking van de gegevens uit de gegevensbanken die daarvoor nodig zijn*;" ».

57. L'Autorité prend acte de ces modifications. L'Autorité attire toutefois l'attention du demandeur sur le fait que celles-ci ne suffisent pas à répondre à l'ensemble des commentaires émis par l'Autorité. Elle relève également par ailleurs au 4° que la partie « *het uitwerken van de technische modaliteiten om de toegangskanalen zo efficiënt en veilig mogelijk uit te bouwen* » apparaît redondante.

### II.3.3. Identification électronique et Règlement eIDAS

58. C'est également l'intégrateur de services qui « *met à disposition des services de connexion électronique pour les applications publiques au sein du service d'authentification, conformément à l'article 9*[31] *de la loi du 18 juillet 2017 relative à l'identification électronique et des applications et systèmes nécessaires au fonctionnement de ce service d'authentification et des systèmes d'identification prévus par le 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* » (souligné par l'Autorité). L'exposé des motifs précise que l'ajout apporté par le Projet « *permet à l'intégrateur de services d'être prêt entre autres pour des interactions avec le portefeuille européen d'identité numérique, pour la mise en correspondance des identités, pour la validation d'attributs,…* » (souligné par l'Autorité). Dans ce contexte, l'Autorité a interrogé le demandeur afin de savoir si l'ajout avait une portée dépassant l'exécution du Règlement eIDAS et de sa réforme et dans l'affirmative, en quoi. Le demandeur a répondu ce qui suit : « *Correct, ils se limitent à anticiper l'exécution de la réforme du Règlement eIDAS* ».

59. **L'Autorité,** qui réserve son analyse sur ce point pour le motif déjà évoqué, est par conséquent d'avis qu'**il convient de se référer explicitement aux services concernés du Règlement eIDAS réformé et aux dispositions qui les prévoient**.

### II.3.4. Règlement n° 2018/1724

60. L'intégrateur de service « *met à disposition les applications et les systèmes d'échange de données pour atteindre les objectifs visés par* » le Règlement 2018/1724.

61. L'Autorité est de nouveau d'avis que **cette disposition devrait se référer aux dispositions pertinentes du Règlement n° 2018/1724** afin de pouvoir identifier précisément ce qu'elle revêt.

### II.3.5. Développement, test, maintien d'applications et systèmes

62. L'article 4, 12°, de la loi de 2012 telle que modifié par le Projet prévoit que l'intégrateur de service « *développe, teste, maintient, corrige et met à disposition les applications et systèmes nécessaires à la réalisation des missions précédentes et traite les données des bases de données nécessaires à cet effet* ». L'exposé des motifs précise à ce sujet que : « *Il est en outre précisé que pour remplir toutes*

[31] Cette disposition est rédigée comme suit :

« *§ 1er. Sans préjudice des obligations liées au Règlement (UE) 910/2014, le Service public fédéral Stratégie et Appui est chargé d'offrir des services d'identification électronique pour des applications publiques au sein du service d'authentification*

*§ 2. Le service public fédéral Stratégie et Appui veille à la disponibilité du service d'authentification.*

*§ 3. Pour l'exécution de sa mission d'authentification, le service public fédéral Stratégie et Appui a le droit d'utiliser le numéro d'identification des personnes physiques inscrites au Registre national* ».

*les missions, l'intégrateur de services doit développer, tester, corriger et mettre à disposition des applications et des systèmes et utiliser les données pertinentes pour ce faire. Il s'agit, dans la mesure du possible, de données de test, si l'utilisateur en dispose, et non de données réelles. Si, à la demande de l'utilisateur, des tests doivent être effectués avec des données réelles, les mesures nécessaires devront être prises pour les protéger conformément* [au] *RGDP* » (souligné par l'Autorité).

63. L'Autorité a interrogé le demandeur quant à la portée et la plus-value d'une telle disposition qui semble dans une certaine mesure au moins, redondante avec les dispositions auxquelles elle se réfère. S'agit-il par exemple d'obliger l'intégrateur de services à développer lui-même (sans recours à la sous-traitance) les applications concernées ? S'agit-il d'encadrer le traitement des données à caractère personnel à des fins de test[32] ? Le demandeur a répondu qu'il ne s'agissait pas d'empêcher le recours à la sous-traitance, ainsi que ce qui suit :

> « ***L'exécution des missions*** *de l'intégrateur de services fédéral* ***suppose un certain nombre de traitements pour lesquels il était approprié de les mentionner explicitement afin d'éviter des discussions relatives aux finalités*** *des traitement, tels que le développement, les tests, la maintenance, la correction et la mise à disposition des applications et des systèmes.*
> *La mention des tests en elle-même est bien-sûr insuffisante pour justifier éventuellement le traitement de données personnelles dans le cadre des tests, mais elle indique clairement que les tests font partie intégrante des missions du SPF BOSA. Pour tout traitement éventuel (et exceptionnel) de données à caractère dans le cadre des tests, tous les principes du RGPD doivent être appliqués, y compris bien sûr le principe de minimisation des données* » (mis en gras par l'Autorité).

64. **L'Autorité ne perçoit toutefois pas la plus-value juridique de l'article 4, 12°, de la loi de 2012 dont la portée reste floue**. En effet, soit pour la réalisation d'une de ses missions, l'intégrateur de service doit mettre en place et en œuvre un système ou une application. Cela implique alors qu'il puisse la développer, la tester, la maintenir. Soit la disposition a pour objectif de permettre des traitements spécifiques de données à caractère personnel et elle est alors bien trop vague, ne déterminant pas les éléments essentiels des traitements qu'elle entend permettre (conformément aux principes de prévisibilité et de légalité rappelés par ailleurs). Telle que rédigée, une telle disposition ne peut avoir d'effet utile quant à la question de savoir si des tests peuvent ou pas être réalisés via des données « réelles »[33] (problématique évoquée dans l'exposé des motifs). Cela va sans dire, elle

[32] Voir à propos du traitement ultérieur de données à caractère personnel à des fins de test, certes dans un autre contexte que celui du secteur public, Sur le traitement de données à caractère personnel à des fins de test, voir CJUE (1re Ch.), arrêt du 20 octobre 2022, *Digi c/ Nemzeti Adatvédelmi és Információszabadság Hatóság*, aff. C-77/21.

[33] Cette question doit être résolue par le responsable du traitement, à l'aune notamment du principe de minimisation des données et du cadre normatif applicable *in concreto* à la mission et au traitement concernés. La disposition en Projet est trop vague et générale pour avoir un effet juridique à cet égard.

pourrait encore moins permettre le traitement de données à caractère personnel dans le cadre du développement de systèmes intelligents ou fondés sur le *data mining*. La question de la manière dont les tests et le développement peuvent être réalisés dépendra du cadre normatif applicable aux missions d'intérêt public pour lesquelles le système concerné est développé. Ainsi, compte-tenu de ce cadre normatif, s'il est nécessaire de traiter des données à caractère personnel pour la réalisation de tests, ce traitement sera permis par le RGPD. Dans ces conditions, **l'Autorité est d'avis que la disposition en projet doit être abandonnée ou développée, l'Autorité réservant son analyse sur cette seconde hypothèse**.

### II.3.6. Règlement sur la Gouvernance des Données

65. L'intégrateur de service « *remplit les rôles de point central d'information et d'organisme compétent pour l'assistance technique visés respectivement dans les articles 8 et 7, 1°* »[34] du Règlement sur la Gouvernance des Données. Cette mission n'appelle pas de commentaire particulier de la part de l'Autorité.

### II.3.7. Echange de données avec les autres intégrateurs de services

66. Enfin, l'article 4, 14°, de la loi de 2012 tel que modifié par le Projet prévoit que l'intégrateur de services réalise l'échange des données avec les autres intégrateurs de services. A ce sujet, l'exposé des motifs énonce ce qui suit : « *L'intégrateur de services échange des données avec les autres intégrateurs de services qui à leur tour organisent l'intégration de services et la mise à disposition intégrée de données. La collaboration se fait également dans le cadre du "G-Cloud", un partenariat qui vise à maximiser la coopération en matière d'infrastructures TIC entre les services publics fédéraux* ». L'Autorité a interrogé

[34] L'intégrateur de services fédéral jouera ainsi un rôle dans le cadre de la mise à disposition des données qui, ne pouvant pas être mise à disposition en vertu de la Directive réutilisation et de sa transposition en droit belge, peuvent néanmoins l'être en vertu des règles de droit belges exécutant le Règlement sur la Gouvernance des données. A propos de la réutilisation des documents du secteur public et de ce Règlement, voir l'avis de l'Autorité n° 143/2023, précité, considérants nos 73 et s. Dans ce contexte, conformément à l'article 7, 4., de ce même Règlement, l'assistance concernée consiste notamment, le cas échéant :

*« a) à fournir une assistance technique en mettant à disposition un environnement de traitement sécurisé pour donner accès à la réutilisation de données;*

*b) à fournir des orientations et une assistance technique sur la meilleure manière de structurer et de stocker les données pour les rendre facilement accessibles;*

*c) à fournir un soutien technique pour la pseudonymisation et à garantir le traitement des données d'une manière qui préserve efficacement le caractère privé, la confidentialité, l'intégrité et l'accessibilité des informations contenues dans les données pour lesquelles la réutilisation est autorisée, notamment les techniques d'anonymisation, de généralisation, de suppression et de randomisation des données à caractère personnel ou d'autres méthodes de préservation de la vie privée à la pointe de la technologie, et la suppression des informations commerciales confidentielles, y compris les secrets d'affaires ou les contenus protégés par des droits de propriété intellectuelle;*

*d) à aider les organismes du secteur public, le cas échéant, à fournir une assistance aux réutilisateurs pour demander le consentement des personnes concernées à la réutilisation ou l'autorisation des détenteurs de données conformément à leurs décisions spécifiques, y compris en ce qui concerne le territoire où le traitement des données est prévu et à aider les organismes du secteur public à mettre en place des mécanismes techniques permettant la transmission des demandes de consentement ou d'autorisation des réutilisateurs, lorsque cela est réalisable en pratique;*

*e) à fournir aux organismes du secteur public une assistance lorsqu'il s'agit d'évaluer l'adéquation des engagements contractuels pris par un réutilisateur en vertu de l'article 5, paragraphe 10* ».

le demandeur sur ce que constituait le « G-Cloud » et sur le cadre normatif applicable à celui-ci. Il a répondu dans un premier temps ce qui suit :

> « *G-Cloud est une initiative conjointe des Services publics fédéraux (SPF), des Institutions publiques de sécurité sociale (IPSS) et des organisations informatiques au sein du gouvernement belge. Il est au service et sous la supervision des institutions participantes. La collaboration entre ces institutions est basée sur leurs compétences en question. Vous trouverez plus d'informations ici : https://www.gcloud.belgium.be/fr/home* ». Dans un deuxième temps, il a encore précisé ce qui suit :
> « *Wij hebben geen informatie over een wettelijk kader van de G-Cloud. De G-cloud wordt enkel informatief vermeld in de memorie van toelichting van dit voorontwerp. We stellen voor om de vermelding van de G-Cloud in de memorie van toelichting te schrappen* » (mis en gras par l 'Autorité).

67. L'Autorité **prend acte de l'intention du demandeur de supprimer de l'exposé des motifs la référence au G-Cloud**. L'Autorité est en outre d'avis que **la référence au G-Cloud** (dont elle n'a pas recherché le cadre normatif) **doit effectivement bien être omise**. Le G-Cloud, auquel le dispositif du Projet ne se réfère pas explicitement (la disposition commentée se réfère quant à elle aux intégrateurs de services, catégorie à laquelle le G-Cloud ne semble *a priori* pas appartenir), apparaît être un sujet à part entière nécessitant une analyse supplémentaire spécifique, sur le plan de la protection des données.

### II.3.8. Article 4, al. 1er, de la loi de 2012 et rôle général de l'intégrateur de services

68. Plus globalement, compte-tenu des développements précédents, l'Autorité est d'avis que l'alinéa 1er de l'article 4 de la loi de 2012 doit être **reformulé afin de tenir compte des nouvelles missions qui sont attribuées à l'intégrateur de services fédéral, et ce, sur la base de concepts clairs ou en tout cas, définis dans le Projet**. Sur ce point par exemple, cet alinéa pourrait être lu comme se référant à un troisième type d'intégration, l'intégration des « *processus de traitement des données* », à côté de l'intégration de données et de l'intégration de services, sans pour autant que la portée concrète de ce concept ne soit définie dans le Projet. Remarque : dans ce cadre, il conviendra également de tenir compte des commentaires suivants relatifs à « l'accord » de l'utilisateur.

### II.4. Caractère facultatif du recours aux services de l'intégrateur de services fédéral

69. Tel que modifié par le Projet, l'article 4 de la loi de 2012 maintient le principe selon lequel **le recours à l'intégrateur de services fédéral n'est pas contraignant** : « *L'intégrateur de services fédéral a pour mission, avec l'accord des utilisateurs et des autres intégrateurs de services, d'intégrer les*

*processus de traitement des données et, dans ce cadre, de donner accès de manière intégrée aux données* » (souligné par l'Autorité). Tel que prévu dans le dispositif de la loi de 2012, la nécessité de cet accord vise l'ensemble des missions de l'intégrateur de services fédéral. L'intervention de ce dernier nécessite par ailleurs la conclusion d'un contrat (d'une convention) conformément à l'article 5, § 2, de la loi de 2012, tel que modifié par le Projet. Autrement dit concrètement, par exemple, les services publics concernés ne devraient pas pouvoir être obligés de recourir aux services de l'intégrateur par la loi de 2012, tout comme les ayants-droits.

70. **L'Autorité a interrogé à ce sujet, le demandeur, et ce notamment quant au régime juridique applicable à cet accord et à sa portée** (*quid* si un service public ne souhaite plus recourir à tout ou partie des services de l'intégrateur de services fédéral ? Quelle est la portée de l'accord donné ?). Elle s'est également interrogée sur **l'interaction entre ce principe et les nouvelles missions de l'intégrateur** (par exemple, pour l'article 4, 10°, tel que modifié par le Projet, concernant l'identification électronique, les services de l'intégrateur seront *a priori* incontournables). La nécessité d'un accord préalable conditionne donc notamment l'application de l'article 8 du Projet.

71. Le demandeur a répondu ce qui suit :

> « *Comme prévu par la loi, l'accord de l'utilisateur est inclus dans une convention d'utilisation ou dans des conditions d'utilisation, en fonction du catégorie d'utilisateur.*
>
> ***Une convention d'utilisation** entre la FOD BOSA et un utilisateur spécifique décrira la collaboration concrète entre les parties, en **mentionnant explicitement les services fournis en question**. Ainsi, **la convention d'utilisation inclut à la fois les droits et les obligations des parties concernées en vertu de la loi de 2012**, ainsi que **les accords supplémentaires nécessaires pour définir les droits, les obligations et les responsabilités**. Concrètement, il s'agit notamment de la description des accords de niveau de service, des dispositions relatives à la piste d'audit (conformément à l'article 14 de la loi de 2012). En ce qui concerne la diffusion de données, l'accord d'utilisation avec le responsable de la source authentique contient également les modalités concrètes du traitement des données personnelles effectué dans le cadre de l'intervention de l'intégrateur de services fédéral. Cela inclut notamment : l'identification de la source de données, la base légale de la compétence du Responsable de la source de données ou le cadre réglementaire de la source de données concernée, les catégories de données à caractère personnel, les catégories de personnes concernées, les bases juridiques de la communication (entre source et destinataire) ou les catégories d'autorisation requises pour cette communication (e.g. protocole, délibération, décision spécifique,…), la nature du traitement par l'intégrateur de services, les canaux d'accès pour la mise à disposition, etc.*

> ***Les services fournis et les modalités d'utilisation de ces services sont donc expressément spécifiés dans l'accord d'utilisation.*** *En cas de cessation de la collaboration en question, l'accord d'utilisation est résilié* » (mis en gras par l'Autorité).

72. **L'Autorité est d'avis que le Projet doit être clarifié quant aux éventuelles limites du caractère non contraignant du recours à tout ou partie des services fournis par l'intégrateur de services fédéral**. Il doit se dégager clairement du Projet que les obligations consacrées dans la loi de 2012 en relation avec les missions de l'intégrateur de services **ne s'appliquent que lorsque l'utilisateur choisit librement de recourir aux services concernés de l'intégrateur de service fédéral**.

73. Très concrètement par exemple, s'agissant de **l'échange de données entre utilisateurs** (et en particulier, autorités publiques ; **mission originelle de l'intégrateur de services**), dans le cadre de **l'article 8 de la loi de 2012**, cela implique que si un utilisateur a recours à un service de l'intégrateur de services en vue d'accéder à une source authentique de données, il n'est pas pour autant obligé de recourir aux autres services de l'intégrateur de services pour accéder aux autres données disponibles via ces services, et qui seraient nécessaires pour cet utilisateur, aux fins de l'exécution de ses missions. C'est dans la convention conclue entre l'utilisateur et l'intégrateur de services que seront identifiées les données auxquelles cet utilisateur pourra accéder, via les services de l'intégrateur. Cette approche prend notamment tout son sens compte-tenu du fait que des données issues de sources non authentiques peuvent également être consultées via l'intégrateur de services.

74. Encore faut-il relever qu'**il ne peut être exclu que le cadre normatif applicable à une autorité publique lui impose de recourir à certains services disponibles via l'intégrateur de service fédéral**[35].

75. **Cette approche de la liberté de l'utilisateur** de recourir aux services de l'intégrateur en exécution de la loi de 2012, sans préjudice de dispositions du rang de loi applicables par ailleurs, **paraît cohérente au regard des missions visées aux 1°** (**sauf** les « attestations de données »), **4°** (**sauf** les « portefeuilles électroniques ») **et 8°, de l'article 4 de la loi de 2012, telle que modifiée par le Projet**.

76. Cela étant précisé, l'Autorité **se demande si le maintien du caractère non contraignant du recours aux services de l'intégrateur demeure pertinent et tenable concernant une partie des nouvelles missions de l'intégrateur de services**. Cette question se pose spécifiquement à

[35] Voir par exemple le considérant n° 47 de l'avis n° 82/2023 du 27 avril 2023 *concernant un avant-projet de loi relatif à la création et la gestion du Federal Learning Account (CO-A-2023-052)*.

l'égard de l'identification électronique et de l'exécution des dispositions de droit européen (soit les **1°** (**uniquement pour** les « attestations de données ») **4°** (**uniquement pour** les « portefeuilles électroniques »), **10°, 11° et 13°,** de l'article 4 de la loi de 2012 telle que modifiée par le Projet).

77. S'agissant de l'identification électronique par exemple, dès lors que le service pertinent apparaît offert par l'intégrateur de service et aucune autre entité, il semble bien que les utilisateurs ne jouissent pas de la liberté de recourir ou non aux services de l'intégrateur dans le cadre de l'identification électronique. S'agissant de l'attestation de données, et bien que l'Autorité réserve son analyse sur la mise en œuvre de la réforme du Règlement eIDAS, la même question se pose : à l'échelle européenne, est-il envisagé de prévoir un rôle incontournable de l'intégrateur de services fédéral ou chaque autorité publique concernée demeurera-t-elle libre en la matière ?

78. Dans ces hypothèses autrement dit et de nouveau, **il conviendrait que le dispositif du Projet explicite la portée de « *l'accord* » que doit donner l'utilisateur**. Plutôt que de disposer de la liberté de recourir ou non aux services de l'intégrateur, il se pourrait plutôt que l'utilisateur **doive conclure une convention avec l'intégrateur de service**.

79. En conclusion, l'Autorité est d'avis que **le dispositif de l'article 8 de la loi de 2012 tel que modifié par le Projet** (ainsi que le cas échéant, l'exposé des motifs) **doit être adapté afin de déterminer clairement quelle est la portée de la liberté des utilisateurs** à l'égard des différentes missions de l'intégrateur de services fédéral.

### II.5. Responsabilités au regard du traitement

#### II.5.1. Responsabilités de l'intégrateur de service et des utilisateurs

80. L'article 15 du Projet fixe les **responsabilités au regard du traitement de données**. L'Autorité rappelle sa pratique d'avis constante selon laquelle une autorité publique (ou une entité privée) est en principe **responsable du traitement de données nécessaire à la mise en œuvre de la mission d'intérêt public qui lui incombe (ou qui relève de l'autorité publique dont elle est investie)[36], ou nécessaire à l'obligation légale qui la lie[37],** en vertu de la norme concernée[38,]

[36] Article 6, 1., e), du RGPD .

[37] Article 6, 1., c), du RGPD .

[38] Voir notamment : avis n° 143/2023 du 29 septembre 2023 *concernant un avant-projet de décret portant assentiment à l'accord de coopération entre la Région wallonne et la Communauté française désignant l'intégrateur de services de la Région wallonne et de la Communauté française et un projet d'accord de coopération relatif à la création du service commun aux Gouvernements Wallon et de la Communauté française, dénommé Banque Carrefour d'échange de données (non soumis à assentiment) (CO-A-2023-375), et concernant un avant-projet de décret portant assentiment à l'accord de coopération entre la Région wallonne et la Communauté française désignant l'intégrateur de services de la Région wallonne et de la Communauté française et un projet d'accord de coopération relatif à la création du service commun aux Gouvernements Wallon et de la Communauté française, dénommé Banque Carrefour d'échange de données (non soumis à assentiment) (CO-A-2023-376)*

**39**. Elle souligne en outre la conformité de cette pratique au récent arrêt de la Cour de justice (3e Ch.), du 11 janvier 2024, *Etat belge c/ Autorité de Protection des Données*, aff. C-231/22, concernant la responsabilité du Moniteur Belge.

81. **L'article 15, al. 1er,** de la loi de 2012 tel que modifié par le Projet **s'inscrit directement dans cette logique**, s'agissant de la responsabilité de l'intégrateur de services, et n'appelle par conséquent pas de commentaire de la part de l'Autorité.

82. **L'article 15, al. 2,** de la loi de 2012 tel que modifié par le Projet quant à lui, dispose que « *Sauf disposition contraire, l'utilisateur visé à l'article 2, 10°, a) à g), qui est responsable de la gestion des sources authentiques ou des sources de données, est responsable du traitement pour les traitements consistant en la collecte, la conservation, la gestion et la mise à disposition des données à caractère personnel contenues dans les sources* » (souligné par l'Autorité).

83. De nouveau, l'Autorité est d'avis que cette disposition **s'inscrit dans la logique de sa pratique d'avis** en matière de responsabilités au regard du traitement de données. Cela étant précisé premièrement, dans un contexte tel que celui en cause, l'identification d'une responsabilité au regard du traitement revient à déterminer un élément essentiel du traitement de telle sorte que seule une **norme du rang de loi** peut y procéder. Autrement dit, la disposition doit s'appliquer **sauf en principe, disposition d'une norme du rang de loi** (loi, décret ou ordonnance) **contraire**. Il s'agit en effet de viser en principe une disposition du rang de loi, dès lors que les services de l'intégrateur fédéral ont vocation également à être à disposition des entités fédérées.

84. Deuxièmement, l'Autorité souligne qu'en principe, **cette responsabilité devrait bien être consacrée dans le** (ou découler clairement du) ***cadre normatif applicable à la source* (authentique ou pas) de données concernée**. L'Autorité comprend néanmoins que le demandeur entende garantir une sécurité juridique supplétive dans le cadre de l'application du dispositif en Projet. Par ailleurs, en particulier dans le contexte des entités fédérées, il ne serait pas exclu non plus que

considérants nos 7 et s. ; avis de l'Autorité n° 83/2023 du 27 avril 2023 *concernant un avant-projet d'ordonnance modifiant l'ordonnance du 4 avril 2019 portant sur la plate-forme d'échange électronique des données de santé (CO-A-2023-147)*, considérant n° 11 ; avis n° 129/2022 du 1er juillet 2022 *concernant les articles 2 et 7 à 47 d'un projet de loi portant des dispositions diverses en matière d'Economie*, considérants nos 42 et s. ; l'avis n° 227/2022 du 29 septembre 2022 *concernant un avant-projet de décret relatif aux données ouvertes et à la réutilisation des informations du secteur public (CO-A-2022-209)*, considérants nos 17-23 ; avis n° 131/2022 du 1er juillet 2022 *concernant un projet de loi portant création de la Commission du travail des arts et améliorant la protection sociale des travailleurs des arts*, considérants nos 55 et s. ; l'avis n° 112/2022 du 3 juin 2022 *concernant un projet de loi modifiant le Code pénal social en vue de la mise en place de la plateforme eDossier*, considérants nos 3-41 et 87-88 ; avis n° 231/2021 du 3 décembre 2021 *concernant un avant-projet d'ordonnance concernant l'interopérabilité des systèmes de télépéage routier*, considérants nos 35-37 ; l'avis n° 37/2022 du 16 février 2022 *concernant un avant-projet de décret instituant la plateforme informatisée centralisée d'échange de données 'E-Paysage'*, considérant n° 22 ; l'avis n° 13/2022 du 21 janvier 2022 *concernant un projet d'arrêté du Gouvernement de la Région de Bruxelles-Capitale relatif à l'octroi de primes à l'amélioration de l'habitat et un projet d'arrêté du Gouvernement de la Région de Bruxelles-Capitale modifiant l'arrêté du Gouvernement de la Région de Bruxelles-Capitale du 9 février 2012 relatif à l'octroi d'aides financières en matière d'énergie*, considérants nos 9-17.

[39] Avis n° 154/2023 du 20 octobre 2023 *concernant un avant-projet de décret et ordonnance conjoints portant le code bruxellois de la gouvernance et de la donnée (CO-A-2023-407)*, considérant n° 167.

dans les interactions avec l'intégrateur de service fédéral, le droit de l'entité fédérée prévoie également une responsabilité additionnelle de son propre intégrateur de service (auquel cas, le responsable de la gestion de la source authentique de données ne serait par exemple plus le seul responsable de la mise à disposition des données).

85. Troisièmement, dans le contexte d'une réforme du droit wallon de l'échange de données issues de sources authentiques, l'Autorité a considéré que la source authentique de données et l'intégrateur de service étaient **responsables conjoints** du traitement de communication des données aux services publics participants[40]. L'Autorité est d'avis que **ces considérations sont valables *mutatis mutandis* dans le cadre du présent Projet**, également à l'égard de sources de données non authentiques mises à dispositions via l'intégrateur de services fédéral.

86. **L'article 9 de la loi de 2012 tel que modifié par le Projet s'inscrit d'ailleurs tout à fait dans cette logique** en prévoyant **une obligation de contrôle de l'intégrateur de services fédéral**. Ainsi, selon cette disposition, « *A chaque requête de consultation ou de communication, l'intégrateur de services fédéral examine si le demandeur et la requête concernée satisfont aux règles de la base de données ou de la source authentique concernée ou aux règles applicables aux systèmes gérés par l'intégrateur de services fédéral dans le cadre de ses missions telles que définies à l'article 4* » (souligné par l'Autorité). **L'Autorité note au passage que l'article 9 de la loi de 2012 devrait être complété afin de préciser les conséquences de cet examen** (ainsi, *a priori*, une demande non conforme sera rejetée) **et le rôle éventuel de la source de données** à laquelle un utilisateur entend accéder.

87. **Dans la même logique, l'article 8, § 2, de la loi de 2012 telle que modifiée par le Projet**, prévoit que « *Si la communication de données à caractère personnel entre utilisateurs dans les conditions légales applicables nécessite un accord ou une autorisation d'une autorité compétente, l'intégrateur de services fédéral communique les données à caractère personnel demandées dans la mesure où un accord ou une autorisation existe, même si l'échange par le biais de l'intégrateur de services fédéral n'y est pas explicitement prévu* » (souligné par l'Autorité). L'Autorité est par ailleurs d'avis que sur ce point, le Projet doit clarifier **qu'il appartient bien à l'intégrateur de services de vérifier, pour toute demande de communication de données, si celle-ci doit faire l'objet ou non d'un tel accord ou d'une telle autorisation**.

88. **L'article 14 de la loi de 2012 tel que modifié par le Projet**, concernant la sécurisation des données, **s'inscrit encore dans cette logique de responsabilité conjointe** en prévoyant une obligation commune à l'utilisateur et à l'intégrateur de services[41].

[40] Voir les considérants nos 12-14 de l'avis n° 143/2023.

[41] Voir les considérants 123 et s.

89. Cela étant précisé**, l'exposé des motifs précise bien qu'il est question de « trois responsables du traitement distincts »**. L'Autorité est d'avis que **le Projet doit être adapté sur ce point.**

90. Le Projet modifie encore **l'article 6 de la loi de 2012** en prévoyant que désormais **le Roi « *peut* » (plutôt que doit,** soit « peur répartir » à la place de « *répartit* »), sans préjudice de la législation spécifique en la matière, répartir fonctionnellement, par arrêté délibéré en Conseil des Ministres, la collecte et le stockage des données authentiques. A ce sujet, l'exposé des motifs précise que « *L'article 6 prévoit que le Roi peut répartir fonctionnellement la collecte et le stockage des données authentiques. Jusqu'à présent, cela n'a pas été fait parce que cela ne s'est pas avéré nécessaire ; cela devrait donc se limiter à une possibilité* » (souligné par l'Autorité). L'Autorité a interrogé le demandeur afin de déterminer si la raison pour laquelle cela n'a pas été nécessaire est liée au cadre normatif applicable par ailleurs. Le demandeur a répondu ce qui suit : « *Correct, cela s'applique uniquement s'il y a une nécessité et qu'il n'existe pas déjà de réglementation en place* ».

91. L'Autorité est d'avis qu'en effet, sur le plan des principes, s'agissant de l'échange de données issues d'une **source authentique de données,** l'article 6 de la loi de 2012 ne devrait en principe jamais avoir à s'appliquer dès lors que **conformément aux principes de prévisibilité et de légalité, les éléments essentiels des traitements de données concernés (notamment la collecte et le stockage) doivent être fixés dans la norme de rang de loi régissant la source authentique concernée**. Autrement dit, **l'Autorité est d'avis que l'article 6 de la loi de 2012 peut être supprimé.**

### II.5.2 Comité de coordination

92. L'Autorité a interrogé le demandeur quant à la portée de l'article 27, al. 3, en projet de la loi de 2012, selon lequel « *Le comité de coordination délibère sur des initiatives visant à promouvoir et à maintenir la collaboration au sein du réseau, et sur des initiatives pouvant contribuer à un traitement légitime et confidentiel des données du réseau* » (souligné par l'Autorité). Est-il envisagé de permettre au Comité de coordination de prendre des décisions contraignantes pour l'intégrateur de services (et le cas échéant ses utilisateurs) dans le domaine du traitement de données à caractère personnel ? Le demandeur a répondu ce qui suit : « *Non, cette compétence n'est pas prévue dans la loi* ». **L'Autorité prend acte de cette réponse et invite le demandeur à clarifier la disposition en Projet qui est floue** quant au rôle du Comité de coordination.

93. L'article 33 actuel de la loi de 2012, prévoit déjà que le Comité de concertation[42] « *délibère sur des initiatives visant à promouvoir et à maintenir la collaboration entre les intégrateurs de services* » (souligné par l'Autorité). Le Projet prévoit en outre que « *Le comité de concertation des intégrateurs de services a pour objectif d'organiser les interconnexions entre intégrateurs de services de manière optimale et efficace afin que les organismes ne doivent s'appuyer que sur un seul intégrateur de services* » (souligné par l'Autorité). L'Autorité a interrogé le demandeur afin d'identifier si et dans quelle mesure il est envisagé que le Comité de concertation prenne des décisions contraignantes pour les intégrateurs de services et/ou les utilisateurs dans le domaine du traitement de données à caractère personnel. Il a répondu ce qui suit : « *Non, cette compétence n'est pas prévue dans la loi* ». L'Autorité prend acte de cette réponse et invite de nouveau le demandeur à **clarifier les dispositions en Projet**. Par ailleurs, elle est d'avis que **l'exposé des motifs doit confirmer que le Comité de coordination n'a pas pour vocation de prendre des décisions contraignantes pour les intégrateurs de services et/ou les utilisateurs dans le domaine du traitement de données à caractère personnel**.

## II.6. Droits des personnes concernées

### II.6.1. Publication de registres par l'intégrateur de services

94. Sur le plan de la transparence**, l'Autorité souligne d'emblée la plus-value apportée par le Projet sur le plan de la protection des données** quant à l'obligation mise à charge de l'intégrateur de services fédéral[43] de mettre à disposition du public le « ***registre intégré des activités de traitement*** »[44] et le « ***registre des sources authentiques*** »[45]. Il s'agit d'outils importants en matière de transparence.

95. Cela étant précisé, **l'Autorité est d'avis que cette mesure de publicité doit être renforcée**. En effet, comme cela a été rappelé précédemment, l'intégrateur de services ne se limite pas à mettre à disposition des données issues de sources authentiques mais il permet également la **mise à disposition de données issues d'autres sources**. Un **registre séparé**, à l'image du registre des

[42] Qui, selon la loi de 2012, se compose d'un représentant de l'intégrateur de services fédéral et d'un représentant des différents autres intégrateurs de services.

[43] Article 4, 9°, de la loi de 2012 telle que modifiée par le Projet.

[44] Soit selon l'article 2, 12°, de la loi de 2012 telle que modifiée par le Projet :

« *une copie intégrée du contenu des registres visés à l'article 30 du règlement (UE) 2016/679 du 27 avril 2016 du Parlement européen et du Conseil 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 et détenus par les utilisateurs visés à l'article 2, 10°, a à g, composée et rendue accessible au public par l'intégrateur de services fédéral* ».

[45] Soit selon l'article 2, 13°, de la loi de 2012 telle que modifiée par le Projet :

« *registre contenant la liste des sources authentiques, la description des données qu'elles comportent et la référence à la législation applicable, composé et rendu accessible au public par l'intégrateur de services fédéral* ».

sources authentiques de données, **devrait également être publié par l'intégrateur de services à ce sujet**.

### II.6.2. Protocoles, conventions d'utilisation, conditions d'utilisation

96. L'article 5, § 2, de la loi de 2012, tel que modifié par le Projet, est rédigé comme suit :

> « *Les modalités d'intervention de l'intégrateur de services fédéral sont fixées dans une convention d'utilisation entre l'intégrateur de services fédéral et les utilisateurs visés à l'article 2, 10°, a) à g), et dans des conditions d'utilisation à l'égard des utilisateurs visés à l'article 2, 10°, h).*
> *En concluant une convention d'utilisation ou en imposant des conditions d'utilisation, l'intégrateur de services fédéral est dispensé de conclure un protocole tel que visé à l'article 20 de la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel* » (souligné par l'Autorité).

97. L'exposé des motifs précise que « *La convention d'utilisation contient les dispositions relatives à la protection des données personnelles ainsi que d'autres dispositions telles que les niveaux de service* ». L'Autorité comprend que le Projet entende en ce sens éviter la multiplication de formalités qui seraient le cas échéant redondantes. Cela étant précisé, et comme le souligne le demandeur lui-même dans les réponses qu'il a communiquées au Conseil d'Etat[46], le Protocole d'une part, nécessite un avis du délégué à la protection des données, et d'autre part surtout, doit être publié.

98. Dans la lignée de l'exposé des motifs (prévoir les dispositions relatives à la protection des données dans les conventions) et dans un souci de transparence, l'Autorité est d'avis que **le Projet ne peut dispenser l'intégrateur de services de conclure des protocoles qu'à la condition suivante.** Celui-ci doit **prévoir que lorsque ces informations sont pertinentes, les conditions d'utilisation et les conventions reprennent les informations du protocole visées à l'article 20, § 1er, al. 2, de la LTD, dans une section dédiée dont la publication est assurée sur le site de l'intégrateur de services**, ce dernier pouvant également mettre à disposition l'intégralité des conventions conclues, dans les limites permises par le RGPD (c'est-à-dire, le cas échéant, moyennant anonymisation préalable, à l'exception de la mention de l'identité des signataires, etc., question à apprécier le cas échéant au cas par cas et avec l'utilisateur concerné). **Ceci est d'autant plus important que c'est dans ces conventions que sera définie la mesure dans laquelle un utilisateur entend recourir aux services de l'intégrateur de services fédéral.**

[46] Pp. 6-7 de l'avis précité.

99. Par ailleurs, l'Autorité rappelle que l'article 38, 1., du RGPD dispose que le « *responsable du traitement et le sous-traitant veillent à ce que le délégué à la protection des données soit associé, d'une manière appropriée et en temps utile, à toutes les questions relatives à la protection des données à caractère personnel* ». L'Autorité est d'avis qu'au même titre que les Protocoles, **l'établissement des conventions et conditions d'utilisation juste évoquées nécessitent l'association du délégué à la protection des données**. Il s'agit d'instruments juridiques centraux au fonctionnement de l'intégrateur de services fédéral.

### II.6.3. Accès et rectification

#### *a) Disposition en projet*

100. Tel que modifié par le Projet, l'article 16 de la loi de 2012 s'énonce comme suit :

> «*§ 1er. Sauf dispositions contraires dans des lois spéciales, toute personne a le droit d'obtenir sans frais la rectification de toute donnée inexacte qui la concerne.*
> *Les requêtes d'adaptation de données sont introduites au moyen des canaux d'accès déterminés par l'intégrateur de services fédéral et les utilisateurs visés à l'article 2, 10°, a) à g).*
> *A chaque requête d'adaptation par le biais de l'intégrateur de services fédéral, l'intégrateur de services fédéral examine si le demandeur et la requête satisfont aux conditions qui sont d'application.*
>
> *§ 2. Toute personne a le droit de savoir quelles autorités et quelles quels organismes ont, au cours des douze mois écoulés, consulté ou mis à jour ses données par le biais du réseau, à l'exception des autorités administratives et judiciaires ou des services chargés de la surveillance ou de la recherche ou des poursuites ou de la répression des délits, de la police fédérale, de la police locale, du Comité permanent de contrôle des services de police et du Comité permanent de contrôle des services de renseignements ainsi que de leur service d'enquêtes respectif, de l'Organe de coordination pour l'analyse de la menace, de la Sûreté de l'Etat, du Service Général du Renseignement et de la Sécurité et de l'Inspection générale de la police fédérale et de la police locale.*
> *L'intégrateur de services fédéral prévoit les moyens techniques appropriés pour assurer l'exécution des accords écrits en application de l'article 14.*
>
> *§ 3. Sans préjudice de la responsabilité des responsables du traitement des bases de données et des sources authentiques, l'intégrateur de services fédéral fournit les moyens techniques aux utilisateurs visés à l'article 2, 10°, a) à g), afin de permettre aux personnes concernées d'exercer leurs droits visés à l'article 15 du règlement (UE) 2016/679 du 27 avril 2016 du*

*Parlement européen et du Conseil 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, vis-à-vis des responsables du traitement des bases de données et des sources authentiques* » (souligné par l'Autorité)[47].

101. L'Autorité est d'avis que la portée de cette disposition, dont le dispositif doit être modifié, **doit être clarifiée**.

***b) Relation avec le RGPD, les dispositions particulières de droit belge et l'article 13 de la loi de 2012***

102. A cet égard **tout d'abord**, et notamment compte-tenu de l'article 23 du RGPD, le dispositif de l'article 16 de la loi de 2012 tel que modifié par le Projet doit explicitement prévoir, dans un premier paragraphe distinct, qu'il est **sans préjudice du RGPD et des lois « particulières »** (et non « spéciales », en se ralliant au commentaire émis par le Conseil d'Etat), **décrets ou ordonnances** (dès lors que le Projet à pour ambition de pouvoir s'appliquer également aux entités fédérées), **qui régissent les droits des personnes concernées dans les limites permises par le RGPD et la LTD**.

103. De cette manière, il sera garanti que la disposition en Projet d'une part, ne peut être lue comme restreignant les droits consacrés dans le RGPD, et d'autre part, ne peut non plus avoir un impact sur les limitations des droits des personnes concernées qui auraient été consacrées par ailleurs en droit belge (et ce, en exécution du RGPD ou de la Directive (UE) n° 2016/680 du Parlement européen et du Conseil du 27 avril 2016 *relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil*).

104. A cet égard, l'Autorité est d'avis que compte-tenu du commentaire précédent, **l'article 13 de la loi de 2012 peut et doit être adapté compte-tenu de la largesse du concept d'utilisateur**. Tel

[47] L'article 16 actuel de la loi de 2012 est rédigé comme suit :

« *§ 1er. Toute personne a le droit d'obtenir sans frais la rectification de toute donnée inexacte qui la concerne. Les requêtes d'adaptation de données sont introduites au moyen des canaux d'accès déterminés par l'intégrateur de services fédéral et les services publics participants.*

*A chaque requête d'adaptation par le biais de l'intégrateur de services fédéral, l'intégrateur de services fédéral examine si le demandeur et la requête satisfont aux conditions établies dans les banques de règles pertinentes.*

*§ 2. Toute personne a le droit de savoir quelles autorités, quels organismes ou quelles personnes ont, au cours des six mois écoulés, consulté ou mis à jour ses données par le biais du réseau, à l'exception des autorités administratives et judiciaires ou des services chargés de la surveillance ou de la recherche ou des poursuites ou de la répression des délits, de la police fédérale, du Comité permanent de contrôle des services de police et du Comité permanent de contrôle des services de renseignements ainsi que de leur service d'enquêtes respectif, de l'Organe de coordination pour l'analyse de la menace, [1 de la Sûreté de l'Etat, du Service Général du Renseignement et de la Sécurité]1 et de l'Inspection générale de la police fédérale et de la police locale.*

*L'intégrateur de services fédéral prévoit les moyens techniques appropriés pour assurer l'exécution des décisions du comité de concertation en application de l'article 14* ».

que modifié par le Projet, celui-ci s'énonce comme suit : « *A défaut de dispositions légales ou réglementaires contraires, l'intégrateur de services fédéral ne confère aux utilisateurs aucun droit complémentaire relatif à la consultation, à la communication ou à tout autre traitement de données en sus des autres dispositions légales et réglementaires applicables* » (souligné par l'Autorité). **L'Autorité est d'avis que cette disposition doit être adaptée pour deux motifs : compte-tenu du fait que désormais, la personne concernée peut être un utilisateur au sens du Projet et afin de clarifier l'ancrage légal des droits conférés aux autres utilisateurs et la limite du rôle de l'intégrateur à cet égard.**

105. Quant à ce second point, **cette disposition est importante** en ce qu'elle rappelle l'effet des principes de prévisibilité et de légalité, en précisant *mutatis mutandis*, que **l'intégrateur de services fédéral ne peut permettre un traitement de données à caractère personnel que si le cadre normatif applicable le permet**.

106. L'Autorité relève d'ailleurs que l'article 13 **ne pourrait pas permettre qu'une disposition réglementaire déroge au principe qu'il fixe**, sauf à violer les principes de prévisibilité et de légalité (consacrés dans des normes de rang supérieur, la Constitution, la CEDH et la Charte). La loi de 2012 ne peut en effet valider indirectement des dispositions réglementaires qui donneraient à l'intégrateur de services fédéral la possibilité de conférer aux utilisateurs des droits relatifs au traitement de données qui ne seraient pas déjà prévus par une norme du rang de loi (conformément aux principes de prévisibilité et de légalité). **L'article 13 doit par conséquent être adapté et supprimer la référence à la norme réglementaire**.

107. Pour mémoire, l'Autorité a interrogé le demandeur quant à la question de savoir s'il existait aujourd'hui, de telles dispositions légales ou réglementaires. Celui-ci a répondu « *Non, mais nous ne pouvons pas exclure que de nouvelles réglementations puissent être ajoutées à l'avenir* ». L'Autorité note que de telles réglementations futures devraient en tout état de cause être conformes aux principes de prévisibilité et de légalité (et partant, fixer les éléments essentiels des traitements de données concernés).

108. Quant au premier point, à l'égard de l'intégrateur de services fédéral et des services qu'il offre, en ce que le Projet porte sur la transparence et les **droits des personnes concernées**, **celui-ci doit en principe avoir une plus-value**. **Des dispositions qui se borneraient à répéter l'application de règles déjà applicables par ailleurs (telles que le RGPD) devraient être omises du Projet**. Autrement dit, et en vertu du Projet lui-même (une disposition légale), la personne concernée est bien supposée jouir de droits supplémentaires en application de celui-ci.

***c) Relation avec les missions de l'intégrateur de services fédéral***

109. **Ensuite**, la disposition en Projet doit être **clarifiée compte-tenu d'une part, des missions de l'intégrateur de services fédéral, et d'autre part, des utilisateurs concernés**. En effet, l'extension des utilisateurs et des missions de l'intégrateur de services fédéral implique **une refonte et une clarification de l'article 16 actuel de la loi de 2012** qui n'avait vocation qu'à s'appliquer à l'échange de données issues de sources authentiques et non authentiques entre services publics participants. Le Projet doit identifier clairement **à l'égard de chacune de ces missions**, **l'effet (la plus-value juridique) de l'article 16 de la loi de 2012** en ce qu'il prévoit l'intervention de l'intégrateur de services fédéral, lorsqu'un tel effet de la disposition en projet est souhaité. Comme l'Autorité vient de le rappeler, la disposition en Projet ne serait pas utile si elle se bornait à rappeler l'application de dispositions applicables par ailleurs.

***d) Commentaire des trois objectifs de la disposition en projet***

110. L'Autorité comprend que la disposition en projet poursuit **trois grands objectifs**, qui appellent les commentaires suivants.

111. **Article 16, § 1er**. Premièrement, il s'agit de permettre la **rectification des données** à la demande de la personne concernée (**§ 1er**). A l'égard de cet objectif, la disposition en projet nécessite les remarques suivantes.

112. Il convient de clarifier dans les alinéas 2 et 3 du paragraphe 1er de l'article 16 en Projet qu'est organisée une possibilité de demande de rectification des données traitées par certains utilisateurs (ceux visés à l'article 2, 10°, a) à g)), à introduire **auprès de l'intégrateur de services fédéral lui-même, à charge pour celui-ci**, le cas échéant, de relayer la requête « *au moyen des canaux d'accès déterminés* » par lui et les utilisateurs (visés à l'alinéa 2). L'essentielle plus-value d'une telle disposition est de permettre à la personne concernée de **s'adresser à un interlocuteur** (responsable du traitement) **central et unique**, à même d'identifier d'où provient la donnée concernée et quels autres utilisateurs la traitent à partir de ses services. L'alinéa 3 de la disposition en projet semble bien traduire cette intention mais son interaction avec l'alinéa 2 n'est pas claire.

113. Par ailleurs, l'alinéa 3 du paragraphe 1er de l'article 16 de la loi de 2012 en Projet n'est pas clair en ce qu'il prévoit qu'à chaque requête d' « adaptation » des données, « *l'intégrateur de services fédéral examine si le demandeur et la requête satisfont aux conditions qui sont d'application* » (souligné par l'Autorité). **Le dispositif doit clarifier le rôle joué par l'intégrateur de services fédéral à l'égard des requêtes qu'il reçoit**. Par exemple, se limite-t-il à vérifier l'identité de la personne concernée ? Il incombe de souligner dans ce cadre qu'*in fine*, **c'est *a priori* au responsable du traitement de la source des données que devrait appartenir le rôle** (le pouvoir) **de se**

**prononcer sur la demande de la personne concernée** (modification ou pas, de la donnée concernée), à moins que le Projet n'entende attribuer un rôle prépondérant à l'intégrateur de services en la matière (mais pour quelle raison ?).

114. **Article 16, § 2**. Le **paragraphe 2** a pour finalité de permettre à la personne concernée de **déterminer de manière centralisée**, via l'intégrateur de services fédéral, **quelles entités ont interagi avec ses données** via les services de l'intégrateur de services fédéral. Plus précisément, sont visées les consultations ou mises à jour « *par le biais du réseau* »[48].

115. L'Autorité a interrogé le demandeur quant à la raison pour laquelle le paragraphe 2 de l'article 16 juste cité, ne se réfère plus aux « *personnes* » qui ont eu accès aux données mais se borne à se référer à des « *autorités* » ou « *organismes* », sans d'ailleurs recourir aux concepts d'utilisateurs et d'intégrateur de services. Le demandeur a répondu ce qui suit :

> « *La divulgation de l'identité des individus (p.e. les collaborateurs des SPF) ayant accès aux données en question par l'intermédiaire des services de l'intégrateur de services fédéral, dans la mesure où l'intégrateur de services fédéral disposerait déjà de ces informations (dans certains cas, l'intégrateur de services fédéral facilite la communication entre la source de données et l'entité consultante, qui gère elle-même la gestion des utilisateurs et des accès, de sorte que l'entité consultante connaît l'identité de l'individu et non l'intégrateur de services fédéral), peut être contraire aux droits et libertés de ces personnes. La mesure dans laquelle l'identité de ces individus peut ou doit être communiquée, p.e. sur base du droit d'accès de la personne concernée dont les données ont été consultées, devra être évaluée à la lumière des principes du règlement général sur la protection des données et nécessitera une décision de la personne responsable du traitement qui a reçu ou consulté les données.*
>
> *Votre remarque relative au recours aux concept d'utilisateurs nous semble correcte. Les mots « quelles autorités et quels organismes »* ***devront être logiquement remplacé par « utilisateurs visés à l'article 2, 10°, a) à g)*** » (mis en gras par l'Autorité).

116. L'Autorité prend acte de cette explication et du fait que **les mots « *autorités* » et « *organismes* » seront remplacés par le mot « *utilisateurs* »**. L'Autorité rappelle que la personne concernée a le droit d'obtenir l'identité des destinataires qui ont consulté (ou modifié en l'occurrence) les données à caractère personnel qui lui sont relatives. Autrement dit, **l'intégrateur de services devra**

[48] L'article 2, 8°, de la loi de 2012 tel que modifié par le Projet définit le réseau comme :
« *l'ensemble des banques de données, sources authentiques, systèmes informatiques et connexions réseau des utilisateurs et de l'intégrateur de services fédéral qui sont interconnectés par le biais de l'intégrateur de services fédéral* ».

**identifier[49] ces <u>responsables du traitement</u>**, à savoir, selon les hypothèses concrètes, une autorité publique, un service particulier d'une autorité publique, voire dans certains cas une personne physique[50], une entité privée chargée d'une mission d'intérêt public, etc. L'accès à **l'identité des personnes physiques préposées** de ces responsables du traitement qui ont effectivement eu accès aux données concernées constitue effectivement une question plus complexe qu'il n'est pas nécessaire d'épuiser ici[51].

117. Si l'Autorité souligne le progrès apporté par le Projet qui prévoit désormais une communication de l'information jusqu'à 12 mois en arrière, à la place de la période de 6 mois actuellement consacrée dans l'article 12 de la loi de 2012, l'Autorité attire l'attention du demandeur sur le fait que l'intégrateur de services fédéral étant bien **responsable du traitement des données nécessaire à l'exercice de ses missions, le RGPD lui impose de communiquer à la personne concernée, à sa demande, l'identité des destinataires qui ont eu accès aux données et ce, <u>sans fixer de période particulière</u>.**

118. L'Autorité est d'avis qu'une **<u>période de 12 mois est trop courte</u>**. Interrogé quant aux critères pris en compte pour déterminer une telle période, le demandeur n'a rien précisé. L'Autorité rappelle que l'article 12, 5., du RGPD régit l'hypothèse dans laquelle la personne concernée adresserait au responsable du traitement des demandes manifestement infondées ou excessives. Et elle est d'avis que la question de savoir sur quelle période la personne concernée peut avoir accès à l'identité des destinataires des données **<u>doit être mise en relation avec la période que doit couvrir l'*audit trail* à mettre en place par le responsable du traitement</u>[52]**, en vertu des principes de sécurité du traitement (mise en place des mesures techniques et organisationnelles, article 32 du RGPD) et de responsabilité du responsable du traitement (article 24 du RGPD). En effet, **<u>aussi longtemps que le responsable du traitement dispose de cette information, la personne concernée doit pouvoir y avoir accès</u>**. Il s'agit en l'occurrence d'une période de **<u>10 ans</u>**.

119. Enfin, s'agissant de **l'exception** prévue par le Projet, l'intégrateur de service fédéral étant un responsable du traitement, **l'information selon laquelle les données ont été communiquées à** des « *autorités administratives et judiciaires ou des services chargés de la surveillance ou de la recherche ou des poursuites ou de la répression des délits, de la police fédérale, de la police locale, du Comité permanent de contrôle des services de police et du Comité permanent de contrôle des services de renseignements ainsi que de leur service d'enquêtes respectif, de l'Organe de coordination pour l'analyse de la menace, de la Sûreté de l'Etat, du Service Général du Renseignement et de la Sécurité et*

[49] Voir par exemple, C.J.U.E. (1re Ch.), arrêt du 12 janvier 2023, *RW c/ Österreichische Post AG*, aff. C-154/21.

[50] L'Autorité a par exemple déjà considéré qu'un chercheur ou un magistrat pouvaient être des responsables du traitement.

[51] Voir par exemple , C.J.U.E. (1re Ch.), arrêt du 22 juin 2023, *J.M.*, aff. C-579/21, considérants nos 73 et s.

[52] Voir le considérant n° 129.

*de l'Inspection générale de la police fédérale et de la police locale* », **ne pourra être omise que si et seulement si *in concreto*, en vertu de la législation applicable, elle ne peut effectivement pas être communiquée**. Ce qui nécessitera de la part de l'intégrateur de services fédéral, une appréciation et *a priori*, la mise en place de mesures techniques et organisationnelles lui permettant d'identifier les traitements visés ou pas par l'exception. La **disposition en projet doit par conséquent être adaptée sur ce point**.

120. **Article 16, § 3**. Enfin, le **paragraphe 3** de la disposition en projet impose à l'intégrateur de services fédéral de **mettre à disposition des utilisateurs un moyen technique pour que les personnes concernées puissent exercer leur droit d'accès auprès d'eux**. L'exposé des motifs du paragraphe 3 de la disposition précitée s'énonce comme suit :

> « *Le paragraphe 3 prévoit que l'intégrateur de services doit fournir les moyens techniques permettant aux citoyens d'exercer, en relation avec les sources authentiques, leur droit d'accès visé à l'article 15 du RGPD. Bien entendu, cela n'est possible que si la personne concernée dispose de ce droit. Cela ne dispense pas les responsables des sources de données et des sources authentiques de leurs obligations et de leur responsabilité à cet égard* » (souligné par l'Autorité).

121. L'Autorité relève tout d'abord que **l'exposé des motifs doit être aligné sur le dispositif du Projet** dès lors que le paragraphe 3 de l'article 16 de la loi de 2012 en projet ne s'applique pas seulement aux sources authentiques de données mais **également aux banques de données qui ne constituent pas des sources authentiques de données**.

122. Elle relève ensuite qu'il s'agit d'une **mission à part entière de l'intégrateur de services fédéral**. Celle-ci devrait par conséquent également être **visée par l'article 4 de la loi de 2012 en projet**.

### II.7. Points divers

#### II.7.1. Sécurisation des données

123. En ce qui concerne la sécurisation des données, l'article 14 de la loi de 2012 tel que modifié par le Projet prévoit que « *Pour chaque échange de données par le biais de l'intégrateur de services fédéral, les éléments suivants sont consignés entre l'utilisateur visé à l'article 2, 10°, a) à g), et l'intégrateur de service fédéral* » (souligné par l'Autorité) : à savoir notamment qui effectue quelle authentification de l'identité, les vérifications et contrôles, et la « *manière dont on vielle à ce qu'une reconstruction complète puisse avoir lieu en cas d'examen, à l'initiative d'une instance ou d'un organe de contrôle concerné ou à la suite d'une plainte, de quelle personne physique a utilisé quel service relatif à quelle personne, quand et à quelles fins* ».

124. L'Autorité a interrogé le demandeur quant à **l'allocation de responsabilités entre l'intégrateur de services et l'utilisateur à cette fin** (qui doit consigner quoi et qui doit déterminer les éléments à consigner). Celui-ci a répondu ce qui suit :« *Il semble impossible de le déterminer à l'avance. Il s'agit d'une* ***obligation commune*** *visant à garantir que les arrangements nécessaires sont pris en fonction du rôle et de la responsabilité de chacun dans l'échange. Ces arrangements sont inclus dans l'accord d'utilisation* » (mis en gras par l'Autorité).

125. L'Autorité comprend par conséquent que les obligations consacrées dans l'article 14 de la loi de 2012 tel que modifié par le Projet, en ce qu'elles concernent le traitement de données à caractère personnel, **relèvent de la responsabilité conjointe de l'intégrateur de services fédéral et de l'utilisateur concerné**[53].

126. Plus globalement, la modification de l'article 14 de la loi de 2012 ne peut être limitée à son alinéa 1er sauf à faire perdre à cette disposition sa cohérence. Avant tout, l'Autorité est d'avis que l'alinéa 1er de l'article 14 de la loi de 2012 en projet doit être **reformulé de manière telle qu'il exprime clairement que ses obligations sont à charge de l'utilisateur et de l'intégrateur de service**.

127. Ensuite, il doit indiquer tout aussi clairement et généralement que, **conformément au droit applicable à l'échange de données concerné**, l'utilisateur et l'intégrateur **déterminent et/ou reprennent** (dans le cas où le droit applicable comporterait déjà des règles en la matière) **dans la convention d'utilisation visée à l'article 5, § 2**, les éléments listés. Le droit applicable à l'échange de données concerné est en effet susceptible de comporter des règles pertinentes en la matière et par ailleurs, le « mode de consultation des données » visé au 5° de l'article 14, doit être sans préjudice notamment, du droit d'accès des personnes concernées.

128. En outre, certains concepts ou passages de l'article 14 tel que modifié par le Projet doivent être **reformulés afin d'être plus clairs**. Ainsi, plutôt que de se référer à des « instances », il doit se référer aux concepts consacrés dans la loi (utilisateur, intégrateur de services). Il ne s'agit par ailleurs pas de déterminer la manière dont « on » veille à ce qu'une reconstruction complète puisse avoir lieu, mais bien la manière dont « **l'intégrateur de services fédéral et l'utilisateur garantissent** » qu'une telle reconstruction puisse être réalisée.

129. Enfin, **l'Autorité souligne l'importance du délai de 10 ans minimum** fixé dans l'article 14, 5°, de la loi de 2012 en projet et déjà d'application actuellement et qui n'est pas remis en question dans le Projet. Compte-tenu des missions de l'intégrateurs de services fédéral, il est fondamental qu'un *audit*

[53] A ce propos, voir les considérants nos 85-88.

*trail* (y compris le *logging* y relatif) d'une opération de traitement puisse être reconstitué pendant une période de 10 ans.

### II.7.2. Pouvoir du Roi visé à l'article 44 de la loi de 2012

130. L'article 44 de la loi de 2012, tel que modifié par le Projet (remplacement des termes « *services publics participants* », par les termes « *utilisateurs* ») prévoit que « *Le Roi peut régler, par arrêté délibéré en Conseil des ministres, les tâches des organes cités au Chapitre 5, ainsi que les modalités ultérieures de la collaboration entre l'intégrateur de services fédéral et les utilisateurs* ». L'Autorité a interrogé le demandeur afin d'identifier si le pouvoir attribué au Roi dans l'article 44 de la loi de 2012 pouvait avoir un impact sur le traitement de données à caractère personnel par l'intégrateur de services et les utilisateurs. Le demandeur a répondu ce qui suit :

> « *Jusqu'à présent, aucun arrêté royal n'a été pris en vertu de l'article 44. Un arrêté royal en vertu de l'article 44 qui pourrait avoir un impact sur le traitement de données à caractère personnel ne serait de toute façon possible que dans le cadre de la délégation en question,* ***ce qui n'est pas prévu en l'espèce*** » (mis en gras par l'Autorité).

131. L'Autorité prend acte de cette réponse et est d'avis que **l'exposé des motifs du Projet doit souligner que l'article 44 de la loi de 2012 qu'il modifie n'a pas pour objectif de déléguer au Roi un pouvoir concernant le traitement de données à caractère personnel**. L'Autorité souligne qu'une telle disposition ne répond pas aux exigences de prévisibilité et de légalité déjà rappelées par ailleurs, et ne pourrait par conséquent fonder le pouvoir du Roi à prendre des arrêtés ayant un impact sur le traitement de données à caractère personnel par l'intégrateur de services fédéral ou ses utilisateurs.

### II.7.3. Conseiller en sécurité de l'information

132. L'Autorité a interrogé le demandeur sur la raison pour laquelle le Projet **supprime l'article 22, al. 2, de la loi de 2012**, selon lequel : « *Le conseiller en sécurité désigné par l'intégrateur de services fédéral sera chargé, en plus des fonctions précitées à l'alinéa 1er, de la sensibilisation relative à la sécurisation des informations des services publics participants* ». Celui-ci a répondu ce qui suit :

> « *L'inclusion de la mission de sensibilisation par le conseiller en sécurité de l'intégrateur de services fédéral concernant la sécurité de l'information des services publics participants (à l'époque) dans la loi de 2012 remonte bien sûr à avant l'entrée en vigueur du RGPD. Depuis lors, il incombe à chaque utilisateur de nommer son propre Délégué à la Protection des Données (DPO), qui est responsable de la sensibilisation au sein de sa propre organisation. Cette mission et cette responsabilité n'appartiennent pas à l'intégrateur de services fédéral.*

*Nous souhaitons bien entendu éviter que cette loi puisse être invoquée pour échapper à sa propre responsabilité* ».

133. **L'Autorité prend acte de la suppression** de la disposition concernée et de la motivation y liée. Elle souligne que si cette disposition était maintenue, elle ne dispenserait en rien les responsables du traitement et délégués à la protection des données des obligations qui leur incombe en vertu du RGPD.

134. Par ailleurs, tel que modifié par le Projet, l'article 20, al. 2, de la loi de 2012 énonce ce qui suit : « *Un conseiller en sécurité de l'information peut occuper la fonction de délégué à la protection des données dans le respect des exigences énumérées à l'article 38, 6°, du* [RGPD] ». Ce conseiller relève « *de l'autorité directe du dirigeant de l'utilisateur ou de l'intégrateur de services fédéral* » comme l'indique l'article 21 de la loi de 2012 tel que modifié par le Projet.

135. Dans ce contexte, l'Autorité s'interroge sur la compatibilité du cumul des rôles de conseiller en sécurité de l'information et de délégué à la protection des données tel que le Projet l'autorise, avec le RGPD. Certes, l'article 38, 6°, du RGPD dispose que le délégué à la protection des données « *peut exécuter d'autres missions et tâches* » que celles qu'il définit mais seulement pour autant que le « *responsable du traitement ou le sous-traitant veillent à ce que ces missions et tâches n'entraînent pas de conflit d'intérêt* ». En l'espèce, la question de l'existence d'un conflit d'intérêts se pose puisque le Projet prévoit que le conseiller en sécurité doit fournir des avis d'expert dans le domaine de la sécurisation des informations, en accordant une attention particulière à la sécurité des données et des réseaux, et qu'il doit mener à bien des missions qui lui sont confiées dans le domaine de la sécurisation des informations. Ces activités sont liées à la détermination des moyens et (sous-)finalités de traitement de données à caractère personnel en matière de sécurité de l'information, de telle sorte qu'*a priori*, charger le délégué à la protection des données de ce rôle additionnel entraîne un conflit d'intérêts[54].

136. Interrogé à ce sujet, le demandeur a répondu ce qui suit :

« *Cet article mentionne seulement la possibilité de cumul en tenant compte de l'article 38, paragraphe 6, selon lequel le responsable du traitement (ou le sous-traitant) veillent à ce que les missions et tâches du DPO n'entraînent pas de conflit d'intérêts. En ce qui concerne les conditions de cumul, toutes les parties concernées doivent bien entendu prendre en compte les décisions de l'APD à cet égard (cfr.*

[54] Pour une hypothèse certes distincte mais dans le cadre de laquelle les principes sont rappelés, voir la décision de la Chambre Contentieuse de l'Autorité n° 141/2021 du 16 décembre 2021, disponible sur https://www.gegevensbeschermingsautoriteit.be/publications/beslissing-ten-gronde-nr.-141-2021.pdf, dernièrement consulté le 24/01/2023, considérants nos 59 et s.

*https ://www.autoriteprotectiondonnees.be/professionnel/rgpd-/delegue-a-la-protection-des-donnees/designation)* ».

137. L'article 20, al. 2, de la loi de 2012 tel que formulé dans le Projet donne néanmoins l'impression qu'*a priori*, le cumul n'engendrera pas de conflits d'intérêts, alors que, comme cela vient d'être évoqué, un tel conflit d'intérêts se présentera vraisemblablement. Pour le reste, la disposition en Projet n'a pas de plus-value juridique à autoriser le cumul envisagé, sous réserve du respect du RGPD : en effet, si le RGPD ne s'y oppose pas, alors le responsable du traitement peut lui-même procéder à une désignation cumulative (sans autorisation spécifique de droit belge) ; si le RGPD s'y oppose, ni le droit belge, ni le responsable du traitement ne peuvent permettre une telle désignation. **Dans ce contexte, l'Autorité est d'avis que le second alinéa 2 de l'article 20 doit être supprimé**.

138. Enfin, l'article 20 en projet prévoit que l'intégrateur de services mais également tous les utilisateurs visés à l'article 2. 10°, a) à g) doivent désigner un conseiller en sécurité. **Cela signifie donc que cette exigence est également susceptible de peser sur des personnes physiques.** Dans ce contexte, l'Autorité est d'avis que le demandeur **devrait préciser les cas dans lesquels il n'est pas obligatoire de désigner un conseiller en sécurité, le cas échéant en visant les personnes physiques dans les hypothèses à déterminer**.

### II.7.4. Extension aux Communautés et Régions

139. Le Projet ajoute à la loi de 2012 un article 46*bis* rédigé comme suit :

> « *Dans les conditions et selon les modalités déterminées par les Régions et Communautés et en concertation avec l'intégrateur de services fédéral, les Régions, les Communautés, les pouvoirs locaux et les organismes qui en dépendent peuvent recourir aux services de l'intégrateur de services fédéral* » (souligné par l'Autorité).

140. L'Autorité a interrogé le demandeur quant à la raison pour laquelle un accord de coopération n'était pas envisagé à cette fin. Elle l'a en outre interrogé quant à ce que constituait la « *concertation* » à mener avec l'intégrateur de services fédéral. Le demandeur a répondu ce qui suit :

> « *La coopération envisagée entre les parties concernées* ***est régie par l'Accord de coopération du 26 août 2013*** *entre les administrations fédérales, régionales et communautaires afin d'harmoniser et aligner les initiatives visant à réaliser un e-gouvernement intégré (Moniteur Belge – Belgisch Staatsblad (fgov.be))* ***La concertation s'inscrit bien entendu dans le cadre de l'élaboration de cet accord de coopération*** *et concerne les modalités opérationnelles nécessaires de la collaboration* » (mis en gras par l'Autorité).

141. Avant tout, l'Autorité **renvoie sur ce point le demandeur aux commentaires émis par le Conseil d'Etat au sujet de la disposition en Projet[55]**. Par ailleurs, l'accord de coopération visé par le demandeur existant déjà, la concertation dans le cadre de son élaboration qui serait visée à l'article 46*bis* ne pourrait avoir lieu. L'Autorité souligne encore que l'accord de coopération évoqué par le demandeur n'aborde pas concrètement les relations entre l'intégrateur de services fédéral et les entités fédérées ainsi que les autorités qui en dépendent[56]. Le Projet doit clarifier la manière dont il entend permettre aux entités fédérées et aux autorités qui en relèvent de recourir aux services de l'intégrateur de services fédéral.

**Conclusion**

**Par ces motifs,**
**L'Autorité est d'avis que**

**1**. Le Projet nécessite la réalisation d'une analyse d'impact relative à la protection des données et il est prématuré de se prononcer quant aux dispositions de droit européen qui ne sont pas encore définitives (**considérants nos 8-11**) ;

[55] Le Conseil d'Etat précise notamment ce qui suit :

« *La portée de l'autorisation qui est ainsi accordée aux Régions, aux Communautés, aux pouvoirs locaux et aux organismes qui en dépendent n'apparaît pas clairement.*

***S'il s'agit simplement d'autoriser ces entités à avoir accès aux données traitées par l'intégrateur de services fédéral moyennant la création d'une habilitation légale en ce sens par les Communautés et les Régions, la disposition ne pose pas de difficultés*** […].

***S'il s'agit plus largement*** *d'autoriser les entités visées à recourir aux services de l'intégrateur de services fédéral au vu de l'ensemble de ses missions précisées par l'article 4 en projet de la loi du 15 août 2012, afin de charger celui-ci de l'exécution de politiques qui leurs sont propres (telles que le développement de solutions informatisées dans le cadre de l'exercice de leurs compétences propres), une telle autorisation requiert le recours à un mécanisme de coopération au sens des articles 92bis ou 92bis/1 de la loi spéciale du 8 août 1980 'de réformes institutionnelles'. (références omises par l'Autorité).*

*Par la voie d'un accord de coopération, les autorités concernées peuvent non seulement décider de créer une institution commune, mais elles peuvent aussi choisir de recourir aux services et institutions d'autres autorités. Il est toutefois requis, dans ce cadre, que l'autorité qui propose ses services et institutions soit elle-même compétente matériellement et territorialement et que les parties respectent le principe du fédéralisme financier*[…].

[…]

***Sans qu'il soit nécessaire de se prononcer sur le fond de cet accord de coopération, la section de législation constate qu'il n'a pas fait l'objet d'un assentiment législatif alors que****, sur le fondement de l'article 92bis, § 1er, alinéa 2, de la loi spéciale du 8 août 1980, pareil assentiment était requis. Il en résulte que, selon la disposition précitée, l'accord de coopération ne produit, actuellement, aucun effet. En conséquence, la disposition en projet n'a pas été examinée plus avant* » (mis en gras par l'Autorité).

[56] Les intégrateurs sont visés aux articles 3, 6°, 5, 5°, de l'accord de coopération. La seule référence à l'intégrateur de services fédéral se trouve dans les « actions communes », à l'article 5, 5°, de l'accord de coopération, prévoyant qu'afin d'atteindre l'objectif visé à l'article 1er de l'accord et la réalisation des composants visés à l'article 4, les Parties s'engagent, dans le respect des compétences propres à chacune, à « *prendre part au comité de concertation pour les intégrateurs de services, prévu dans la loi du 15 août 2012 relative à la création et à l'organisation d'un intégrateur de services fédéral* ». L'article 3, 6°, prévoit le principe d' « *une collaboration constructive et des accords clairs entre les intégrateurs de service existants et futurs* ».

**2**. Si le demandeur a renoncé dans le cadre de la mise en état du Projet, à modifier le concept de source authentique de données consacré dans la loi de 2012, le Projet tel qu'il a été soumis à l'Autorité appelle néanmoins certains commentaires. En outre, le Projet doit distinguer clairement l'échange de données issues de sources authentiques de l'échange de données qui ne sont pas issues de sources authentiques (**considérant nos 12-22**) ;

**3.** Quant à la désignation des sources authentiques de données le Projet doit maintenir le principe du droit positif selon lequel un arrêté royal délibéré en Conseil des ministres est nécessaire, plutôt qu'une décision du Comité de coordination. Le Projet apporte une plus-value en matière de protection des données en fixant dans la loi, les critères de désignation des sources authentiques, critères qui devraient être affinés (**considérants nos 23-32**).

**4.** S'agissant des utilisateurs au sens du Projet, la définition visée à l'article 10, 2°, de la loi de 2012 tel que modifié par le Projet doit être modifiée afin d'en assurer la cohérence, et l'article 46 du Projet doit être adapté afin d'une part, d'avoir la portée qui lui est reconnue par le demandeur, et d'autre part, d'être mis en conformité avec les principes de prévisibilité et de légalité (**considérants nos 33-42**) ;

**5.** S'agissant des missions de l'intégrateur de services fédéral, l'alinéa 1er de l'article 4 de la loi de 2012 doit être adapté notamment compte-tenu des nouvelles missions de l'intégrateur. Le dispositif du Projet doit se référer clairement aux dispositions pertinentes des règles de droit européen qu'il entend compléter ou exécuter. Les différentes missions de l'intégrateur de services fédéral doivent être clairement distinguées dans le dispositif du Projet. Le Projet doit définir les opérations de traitement que peuvent permettre de réaliser les applications réutilisables et clarifier si celles-ci peuvent être mises à disposition sous la forme de services. L'article 4, 12°, de la loi de 2012 telle que modifiée par le Projet ne semble pas avoir de plus-value juridique. L'Autorité prend acte de l'intention du demandeur de supprimer la référence au « G-Cloud » dans l'exposé des motifs (**considérants nos 43-68**) ;

**6.** L'Autorité est d'avis que le Projet doit développer la portée de la règle selon laquelle l'intégrateur de services offre ses services avec l'accord de l'utilisateur, et ce également à l'égard des nouvelles missions de l'intégrateur. Le Projet doit clairement identifier quelle est la liberté de l'utilisateur notamment dans l'accès aux données disponibles via l'intégrateur de services (**considérants nos 69-79**) ;

**7.** S'agissant de la fixation des responsabilités au regard du traitement de données, le Projet s'inscrit directement dans la pratique d'avis de l'Autorité, sous réserve de l'identification de responsabilités conjointes au regard du traitement de données, en particulier s'agissant de

l'échange de données entre autorités publiques via les services de l'intégrateur. L'article 15 de la loi de 2012 tel que modifié par le Projet doit également être modifié afin d'être conforme aux principes de prévisibilité et de légalité en vertu desquels par ailleurs, l'article 6 de la loi de 2012 tel que modifié par le Projet devrait être supprimé. L'article 14 du Projet doit préciser les conséquences de l'examen à mener par l'intégrateur de services en cas de requête de consultation ou communication de données, et le rôle éventuel de la source des données (**considérants nos 80-91**) ;

**8.** La compétence de délibération du Comité de coordination doit être clarifiée et l'exposé des motifs du projet doit rappeler que l'article 33 de la loi de 2012 n'a pas pour objet de permettre au Comité de coordination de prendre des décisions contraignantes à l'égard du traitement de données à caractère personnel (**considérants nos 92-93**) ;

**9.** Le Projet apporte une plus-value sur le plan de la protection des données en renforçant la transparence dans le fonctionnement de l'intégrateur de services. Il devrait également prévoir la communication dans un registre séparé, des sources non authentiques de données accessibles via les services de l'intégrateur (**considérants nos 94-95**) .

**10.** Si le Projet peut dispenser l'intégrateur de services de conclure les protocoles visés à l'article 20 de la LTD, l'Autorité est d'avis que c'est à la condition que les conventions à conclure dans le cadre de l'accès aux services de l'intégrateur devraient reprendre les éléments des protocoles visés par la LTD et que les sections y dédiées à tout le moins, devraient être publiées. Le délégué à la protection des données devra par ailleurs être associé à la rédaction des conventions et conditions d'utilisation (**considérants nos 94-99**) ;

**11.** L'article 16 de la loi de 2012 telle que modifiée par le Projet, concernant les droits de rectification et d'accès des personnes concernées, doit être adapté. Il doit préciser qu'il est sans préjudice du RGPD et des lois particulières, décrets ou ordonnances, applicables par ailleurs en droit belge. L'article 13 de la loi de 2012 telle que modifiée par le Projet doit être adapté compte-tenu du fait que la personne concernée peut être un utilisateur, et afin d'être mis en conformité aux principes de prévisibilité et de légalité. Le Projet doit encore clarifier l'application de l'article 16 précité à l'aune des différentes missions de l'intégrateur de services.

Les trois paragraphes de cette disposition appellent certaines clarifications et précisions. Notamment, l'exception prévue est trop large et la communication de l'identité des utilisateurs destinataires des données par l'intégrateur de services fédéral ne peut être limitée aux 12 mois précédant la demande mais doit être étendue à 10 ans (**considérants nos 101-122**) ;

**12.** En ce qui concerne la sécurisation des données, l'article 14 de la loi de 2012 tel que modifié par le Projet doit être adapté notamment afin de préciser à qui incombent les obligations qu'il consacre (**considérants nos 123-129**) ;

**13.** L'exposé des motifs du Projet doit souligner que l'article 44 de la loi de 2012 qu'il modifie n'a pas pour objectif de déléguer au Roi un pouvoir concernant le traitement de données à caractère personnel (**considérants nos 130-131**) ;

**14.** La disposition selon laquelle le conseiller en sécurité de l'information peut également être délégué à la protection des données doit être omise et le Projet devrait prévoir une exception à l'obligation de désigner un conseiller en sécurité de l'information, lorsque l'utilisateur concerné est une personne physique (**considérants nos 132-138**) ;

**15.** Le Projet doit être clarifié quant à la manière dont il entend permettre aux entités fédérées et aux autorités qui en relèvent de recourir aux services de l'intégrateur de services fédéral (**considérants nos 139-141**).

Pour le Centre de Connaissances,
Cédrine Morlière, Directrice

Autorité de protection des données
Gegevensbeschermingsautoriteit

**Advies nr. 24/2024 van 18 maart 2024**

**Betreft: Voorontwerp van wet tot wijziging van de Wet houdende oprichting en organisatie van een federale dienstenintegrator (CO-A-2023-554)**

**Vertaling**[1]

Het Kenniscentrum van de Gegevensbeschermingsautoriteit (hierna genoemd "de Autoriteit"),
Aanwezig: Juline Deschuyteneer, Cédrine Morlière, Nathalie Ragheno, Griet Verhenneman, Yves-Alexandre de Montjoye, Bart Preneel en Gert Vermeulen ;

Gelet op de wet van 3 december 2017 *tot oprichting van de Gegevensbeschermingsautoriteit, en* met name op de artikelen 23 en 26 (hierna "WOG" genoemd);

Gelet op artikel 25, lid 3, van de WOG, op grond waarvan de besluiten van het Kenniscentrum worden genomen bij meerderheid van stemmen ;

Gelet op Verordening (EU) 2016/679 *van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG* (hierna "AVG");

Gelet op de wet van 30 juli 2018 *betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens* (hierna "WVG");

Gelet op de op 7 december 2023 ontvangen adviesaanvraag van de staatssecretaris voor Digitalisering, belast met Administratieve Vereenvoudiging, Privacy en de Regie der gebouwen, , toegevoegd aan de eerste minister, de heer Mathieu Michel (hierna "de aanvrager");

[1] Voor de oorspronkelijke versie van de tekst, die collegiaal werd gevalideerd, cf. de Franse versie van de tekst, die beschikbaar is in de FR-versie van de rubriek "adviezen" van de website van de Autoriteit.

Gelet op de toezending van het verzoek om advies door de Autoriteit, op 12 januari 2024, aan het Controleorgaan op de Politionele Informatie (het COC), het Vast Comité van Toezicht op de inlichtingen- en veiligheidsdiensten (het CTIVD) en het Vast Comité van Toezicht op de politiediensten (het Comité P), overeenkomstig artikel 54/1 van de WOA en het Samenwerkingsprotocol tussen de Belgische federale toezichthoudende autoriteiten op het vlak van dataprotectie, overeengekomen op 24 november 2020;

Gelet op het antwoord van het COC van 7 februari 2024, waarin staat dat het COC geen advies zal uitbrengen;

Gelet op het feit dat de CTIVD op het moment van schrijven nog niet heeft bevestigd of ze een advies zal uitbrengen;

Gelet op het feit dat het Comité P op het moment van schrijven nog niet heeft bevestigd of ze een advies zal uitbrengen;

brengt op 18 maart 2024 het volgende advies uit:

## I. Doel en achtergrond van de adviesaanvraag

1. De aanvrager heeft bij de Autoriteit een adviesaanvraag ingediend betreffende Voorontwerp van wet tot wijziging van de Wet houdende oprichting en organisatie van een federale dienstenintegrator (CO-A-2023-554 (hierna "**het Wetsontwerp**"). Het Wetsontwerp wijzigt de wet van 15 augustus 2012 betreffende de *oprichting en organisatie van een federale dienstenintegrator (*hierna "**de wet van 2012"**).

2. De memorie van toelichting bij het Wetsontwerp verklaart dat het doel ervan onder meer is om rekening te houden met wijzigingen in andere wetgeving, om verbeteringen aan te brengen in de wet van 2012 die voortvloeien uit de praktijk en de geleerde lessen, en de terminologie van de AVG op te nemen in deze wet . Het Wetsontwerp beoogt bepaalde definities te verduidelijken en de rol van de dienstenintegrator, de deelnemende overheidsdiensten en de authentieke gegevensbronnen vast te stellen met betrekking tot de verwerking van persoonsgegevens.

3. Het Wetsontwerp maakt ook deels deel uit van de Europese wetgeving. Zo "neemt het in overweging" Verordening (EU) nr. 2022/868 van het Europees Parlement en de Raad van 30 mei 2022 *Europese datagovernance en tot wijziging van Verordening (EU) 2018/1724 (Datagovernanceverordening)* (hierna "**de Datagovernanceverordening**" of "DGA"), om de federale dienstenintegrator in staat te

stellen bij te dragen aan dit dispositief. Het verduidelijkt ook een taak van de dienstenintegrator in deze context.

4. Het Wetsontwerp "complementeert" Richtlijn (EU) nr. 2019/1024 van het Europees Parlement en de Raad van 20 juni 2019 *inzake open data en het hergebruik van overheidsinformatie (herschikking) (*hierna: "**de Richtlijn hergebruik**"), rekening houdend met het feit dat momenteel "*de federale dienstenintegrator het portaal levert waar open data worden gepubliceerd*", "*verankert het de verstrekking van dit soort informatie door de federale dienstenintegrator*".

5. Bovendien anticipeert het Wetsontwerp ook **op de lopende hervorming** van Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad van 23 juli 2014 *betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG* (hierna: "**de eIDAS-verordening**"), voor wat betreft de "*portemonnee voor digitale identiteit*". Het heeft ook betrekking op de eIDAS-verordening en de wet van 18 juli 2017 betreffende elektronische identificatie (hierna "**de eIDAS-wet**" genoemd), aangezien deze normen momenteel van kracht zijn.

6. Tot slot geeft het Wetsontwerp ook uitvoering aan Verordening (EU) nr. 2018/1724 van het Europees Parlement en de Raad van 2 oktober 2018 *tot oprichting van één digitale toegangspoort voor informatie, procedures en diensten voor ondersteuning en probleemoplossing en houdende wijziging van Verordening (EU) nr. 1024/2012* (hierna "**Verordening 2018/1724**" genoemd).

## II. Onderzoek

Dit advies is als volgt opgebouwd:

## II.1 Relevante adviezen van de Autoriteit, reikwijdte van het Wetsontwerp en reikwijdte van dit advies

7. In verschillende recente adviezen heeft de Autoriteit de gelegenheid gehad om haar beleid met betrekking tot de uitwisseling van gegevens afkomstig uit authentieke (of niet-authentieke) bronnen te herhalen. Daarom dient voorafgaand te worden verwezen naar de **volgende adviezen van de Autoriteit**:

- Advies nr. 154/2023 van 20 oktober 2023 *betreffende een gezamenlijk voorontwerp van decreet en ordonnantie houdende het Brussels Wetboek voor governance en gegevensbeheer (CO-A-2023-407)* (met name overwegingen 46-72) (hierna "**advies nr. 154/2023**");

- Advies nr. 143/2023 van 29 september 2023 *betreffende een voorontwerp van decreet houdende instemming met het samenwerkingsakkoord tussen het Waals Gewest en de Franse Gemeenschap tot aanwijzing van de dienstintegrator van het Waals Gewest en de Franse Gemeenschap en een ontwerp van samenwerkingsakkoord met betrekking tot de oprichting van de gemeenschappelijke dienst van de Advies 154/2023 - 6/80 Waalse Regeringen en de Franse Gemeenschap, genaamd Banque Carrefour d'échange de données (niet onderworpen aan instemming) (CO-A-2023-375), en betreffende een ontwerp van decreet houdende instemming met het samenwerkingsakkoord tussen het Waals Gewest en de Franse Gemeenschap tot aanwijzing van de dienstintegrator van het Waals Gewest en de Franse Gemeenschap en een ontwerp van samenwerkingsakkoord met betrekking tot de oprichting van de gemeenschappelijke dienst van de Waalse Regeringen en de Franse Gemeenschap, genaamd Banque Carrefour d'échange de données (niet onderworpen aan instemming) (CO-A-2023-376) (hierna «advies 143/2023»)* .

8. De Autoriteit merkt op dat het Wetsontwerp **de wet van 2012, die het centrale dispositief vormt van het federale recht met betrekking tot, in het bijzonder, de authentieke gegevensbronnen, aanzienlijk wijzigt**. Zoals de Raad van State aangeeft in zijn advies[2] , waarbij hij betreurt dat de Autoriteit gelijktijdig is geraadpleegd, betreft dit ontwerp "bij uitstek de verwerking *van persoonsgegevens*". In het bijzonder:

   - Het Wetsontwerp breidt het toepassingsgebied *ratione personae* van de wet van 2012 aanzienlijk uit door het begrip "*deelnemende overheidsdienst*" te vervangen door het veel bredere begrip "*gebruiker*";

   - Het wijzigt het begrip van "*authentieke gegevensbron*"[3] evenals de regels volgens welke gegevensbronnen als zodanig worden gekwalificeerd;

   - Het kent nieuwe taken toe aan de federale dienstenintegrator, wiens diensten ook toegankelijk zullen zijn voor de Gemeenschappen, Gewesten, lokale overheden en hun afhankelijke organen;

   - Het behandelt de verantwoordelijkheid van de federale dienstenintegrator en zijn gebruikers, evenals de rechten van de betrokkenen in deze context;

[2] E.C., advies nr. 75.185/2 van 13 februari 2024 over een "*wetsontwerp tot wijziging van de wet betreffende de oprichting en de organisatie van een federale dienstenintegrator*".

[3] Zelfs als de aanvrager er tijdens de voorbereiding van het dossier van heeft afgezien om dit begrip te wijzigen.

- Het verduidelijkt niet de reikwijdte van bepaalde belangrijke bepalingen van de wet van 2012 die onduidelijk zijn, zoals de bepalingen met betrekking tot het niet-bindende karakter van het gebruik van de diensten van de federale dienstenintegrator ;

- Tot slot implementeert het Wetsontwerp bepalingen van Europees recht en anticipeert het op de uitvoering van Europese regels die nog niet zijn aangenomen (het Wetsontwerp zelf is op dit punt onderhevig aan verandering[4] ).

9. In deze context heeft de Autoriteit de aanvrager gevraagd naar de realisatie van een effect**beoordeling inzake gegevensbescherming**. De aanvrager antwoordde als volgt:

> ***"Er is geen effectbeoordeling inzake gegevensbescherming uitgevoerd na het opstellen van de voorgestelde wetswijziging.***
> *De bovenvermelde wijzigingen zullen uiteraard effect hebben op de verwerking van persoonsgegevens door de dienstenintegrator. De FOD BOSA hecht het grootste belang aan de bescherming van natuurlijke personen bij de verwerking van persoonsgegevens. De eigenlijke verwerking van persoonsgegevens in het kader van de uitbreiding van gebruikerscategorieën, de uitbreiding van mogelijke authentieke bronnen en de nieuwe taken zal daarom onderworpen worden aan een effectbeoordeling inzake gegevensbescherming, zoals vereist in artikel 35 van de AVG*" (vetgedrukt door de Autoriteit).

10. Gezien de reikwijdte van het Wetsontwerp[5] **is de Autoriteit van mening dat deze moet worden vergezeld van een effectbeoordeling inzake gegevensbescherming**, zodat er een geïnformeerd en doeltreffend parlementair debat over kan plaatsvinden. Een dergelijke beoordeling zal met name helpen om de oorspronkelijke missie van de federale dienstenintegrator duidelijk te scheiden van zijn nieuwe taken, de reikwijdte van de uitbreiding van de gebruikers van de dienstenintegrator te evalueren, en de noodzakelijke aanpassingen aan het huidige dispositief van de wet van 2012 (opgesteld in een tijd dat de AVG nog niet bestond en de rol van de dienstenintegrator beperkter was) te benadrukken. Een dergelijke analyse zou het ook mogelijk moeten maken om de criteria en de methode voor het identificeren van authentieke gegevensbronnen te evalueren, in een bredere context van het aanbieden van de diensten van de federale dienstenintegrator ook aan deelentiteiten en de overheidsinstanties die van hen afhankelijk zijn (inclusief overwegingen over een nationale samenwerkingsovereenkomst hierover, die het gebruik van zowel federale als regionale authentieke bronnen omvat en ervoor zorgt dat de consistentie op dit gebied wordt gewaarborgd).

[4] Zie het antwoord van aanvrager dat is opgenomen in overweging nr. 14.

[5] Zie overweging 8.

11. Tenslotte, aangezien de **hervorming van de eIDAS-verordening ten** tijde van de opstelling van het Wetsontwerp[6] nog niet is goedgekeurd, is de Autoriteit van oordeel dat het Wetsontwerp, in afwachting van de tenuitvoerlegging van deze hervormde verordening, zich niet in een definitief ontwerpstadium bevindt[7] en dat de **raadpleging van de Autoriteit over dit aspect van het project voorbarig is**. Met andere woorden, de Autoriteit **houdt haar analyse van de tenuitvoerlegging van de hervormde eIDAS-verordening aan en zal zich beperken tot het uitbrengen van de nodige opmerkingen met betrekking tot andere aspecten van de wijziging van de wet van 2012**.

## II.2 Authentieke en andere gegevensbronnen

### II.2.1. Definities

12. In het positief recht wordt het begrip "*authentieke bron*" indirect gedefinieerd via de - verwante - definitie van het begrip "*authentieke gegevens*". Het begrip "*authentieke bron*", dat is vastgelegd in artikel 2, lid 6, van de wet van 2012, is gewijzigd door artikel 2 van het Wetsontwerp. Het begrip "*authentieke gegevens*", dat is vastgelegd in artikel 2, lid 5, van dezelfde wet, blijft daarentegen ongewijzigd[8] . In plaats van een "*databank waarin authentieke gegevens worden opgeslagen*" wordt de authentieke bron voortaan gedefinieerd als "*een register of systeem, onder de verantwoordelijkheid van een publiekrechtelijke of private entiteit, dat kenmerken bevat met betrekking tot een natuurlijke of rechtspersoon en dat wordt beschouwd als de primaire bron van die informatie of als authentiek wordt erkend krachtens het Unierecht of het nationale recht, met inbegrip van het bestuurlijk handelen*" (onderstreping door de Autoriteit).

13. De memorie van toelichting beperkt zich tot het verduidelijken dat de "*definitie van authentieke bron in overeenstemming is gebracht met de definitie zoals vervat in de voorstellen tot wijziging van de eIDAS-verordening*", terwijl **de nieuwe benadering die door het Wetsontwerp wordt geïntroduceerd een aanzienlijke vaagheid introduceert met betrekking tot de reikwijdte van het begrip authentieke gegevensbron**.

14. In deze context heeft de Autoriteit de aanvrager verzocht het doel en de reikwijdte van de wijziging van de definitie van het begrip authentieke gegevensbron toe te lichten (het gebruik van het begrip "*kenmerk"*, het afschaffen van de verwijzing naar "*authentieke gegevens*", *hoe zit het met de*

[6] Op verzoek van de Autoriteit heeft de aanvrager de laatste beschikbare versie van de tekst ingediend, d.w.z. een document van 211 bladzijden in het Engels (zonder gelijkwaardige concepten in het Frans of het Nederlands), met de wijzigingen die zijn aangegeven in de follow-up van de wijzigingen en met referentie PE-CONS 68/23 - 2021/0136 (COD).

[7] Zie voetnoot nr. 4.

[8] Met andere woorden: "*gegevens die door een instantie worden verzameld en beheerd in een databank die authentiek is als unieke en originele gegevens betreffende de betrokken persoon of het betrokken rechtsfeit, zodat andere instanties dezelfde gegevens niet opnieuw hoeven te verzamelen*".

verwijzing naar "*bestuurlijk handelen*", enz. De aanvrager heeft in eerste instantie als volgt geantwoord:

> *"De definitie van authentieke bron in het Wetsontwerp is* ***afgestemd op de definitie die (destijds) was opgenomen in de voorgestelde wijzigingen van de eIDAS-verordening****.*
> *In de laatste versie van het Wetsontwerp tot wijziging van de eIDAS-verordening (zie bijlage, die in februari 2024 ter stemming aan het* ***Europees Parlement zal worden voorgelegd. De stemming in de Raad volgt daarna****), is de volgende definitie opgenomen: 'authentic source' means a repository or system, held under the responsibility of a public sector body or private entity, that contains and provides attributes about a natural or legal person or object and that is considered to be a primary source of that information or recognised as authentic in accordance with Union or national law, including administrative practice".*
> ***We zullen natuurlijk moeten zorgen dat we ons conformeren aan de allerlaatste definitie****.*
>
> *In de laatste versie van het Wetsontwerp tot wijziging van de eIDAS-verordening wordt "kenmerk" als volgt gedefinieerd: "attribute" means a characteristic, quality, right or permission of a natural or legal person or of an object;".*
>
> ***Een bron kan zowel authentieke als niet-authentieke gegevens bevatten. Daarom is het essentieel om de definitie en het begrip van authentieke gegevens in artikel 27 te behouden****.*
>
> ***In antwoord op de opmerking van de Raad van State dat het coherent zou zijn om het verband tussen de definities van "authentieke bron" en "authentieke gegevens" te handhaven, is voorgesteld om de definitie van authentieke bron als volgt te verbeteren****:*
> *"een register of systeem, onder de verantwoordelijkheid van een publiekrechtelijke instantie of een private entiteit, dat kenmerken bevat met betrekking tot een natuurlijke of rechtspersoon en dat wordt beschouwd als de primaire bron van deze authentieke gegevens of als authentiek is erkend krachtens de nationale wetgeving*" (vetgedrukt door de Autoriteit).

Na opnieuw te zijn bevraagd over het begrip van de authentieke bron, heeft de aanvrager in tweede instantie het volgende verduidelijkt:

> *" We stellen voor om naar aanleiding van uw vragen en de vragen van de Raad van State* ***de definities te laten zoals ze bestaan in de huidige wet****.* ***Deze definities zijn geenszins***

***in tegenspraak met de definities in de eIDAS verordening***. *Ze wijzigen levert andere problemen op in de wet omdat de link met authentieke gegevens moet blijven bestaan. Niet elke bron bevat enkel authentieke gegevens, soms zijn er in één bron authentieke en niet authentieke gegevens. Daarom voorziet het gewijzigde artikel 27 het kwalificeren van de gegevens en niet automatisch van de gehele bron* " (vetgedrukt door de Autoriteit).

15. **De Autoriteit neemt er kennis van dat de Aanvrager ervoor kiest om het begrip authentieke bron zoals het momenteel in de wet van 2012 staat niet te wijzigen**. Verder maakt zij de volgende opmerkingen.

16. **Ten eerste** is de Autoriteit van mening dat **het Wetsontwerp ervoor moet zorgen dat het dispositief van de wet van 2012 een duidelijk onderscheid maakt tussen de uitwisseling van gegevens uit authentieke gegevensbronnen en de uitwisseling van gegevens die *niet afkomstig zijn* uit authentieke gegevensbronnen**. In dit opzicht is de logica waarbij overheidsinstanties de gegevensbron **moeten** gebruiken die beschikbaar is via de federale dienstenintegrator, gerechtvaardigd in termen van de beginselen van doelgerichtheid en gegevenskwaliteit, wanneer deze gegevensbron authentiek is. Het is **omwille van de authenticiteit van de gegevens dat het, op basis van deze beginselen, relevant is om andere overheidsinstanties te verplichten om de betrokken gegevensbron te gebruiken**[9] . Deze logica komt niet naar voren uit de bepalingen van de wet van 2012[10] , zodat hergebruik van gegevens tussen overheden *uiteindelijk* kan worden georganiseerd zonder dat er juridisch gebruik wordt gemaakt van authentieke gegevensbronnen. Deze overwegingen houden ook rechtstreeks verband met de vraag naar de reikwijdte van de verplichtingen van een gebruiker (deelnemende overheidsdienst) die gebruik maakt van de diensten van de federale dienstenintegrator[11] .

---

[9] Zie ook overweging 48 van advies nr. 154/2023 van de Autoriteit, die als volgt luidt (referenties weggelaten, vet en onderstreept in de oorspronkelijke tekst):

*" De Autoriteit is van mening dat **deze bepalingen**, wat de beginselen betreft, **het juridische paradigma omkeren dat momenteel van toepassing is op de verwerking van persoonsgegevens naar Belgisch recht, in overeenstemming met de beginselen van rechtmatigheid en voorzienbaarheid** die zijn vastgelegd in artikel 8 EVRM en artikel 22 van de Grondwet. Op die manier **zet het Project de logica van de verwerking van gegevens uit authentieke gegevensbronnen om in elke gegevensuitwisseling waarbij een Brusselse overheidsinstantie partij is**[...] , op voorwaarde dat ze daartoe een memorandum van overeenstemming sluiten*[...] *. Hoewel persoonsgegevens in principe en in alle gevallen **alleen mogen worden** verwerkt **wanneer daar een rechtsgrondslag voor is in het kader van een bevoegdheid of verplichting die aan een overheidsinstantie is toegekend** (bijna altijd in het kader van gegevensverwerking door overheidsinstanties vindt gegevensverwerking plaats in de gevallen bedoeld in artikel 6, lid 1, onder c) en d)).(c) en d)) en dat de **wezenlijke bestanddelen** ervan **worden bepaald door een verordening met de status van wet**, met dien verstande dat, afhankelijk van de betrokken gegevensverwerking, het kader dat wordt geboden door een verordening met de status van wet **meer of minder uitgebreid** zal zijn*[...] *. Met andere woorden, om gegevensverwerking mogelijk te maken is het niet voldoende dat er geen specifieke bepaling is die zich ertegen verzet .*

[10] Zie artikel 4 van de wet van 2012, dat in het algemeen verwijst naar geïntegreerde toegang "*tot gegevens*". Artikel 8 van de wet van 2012, en met name lid 3, is ook van toepassing, ongeacht of de gegevens die via de dienstenintegrator beschikbaar zijn, afkomstig zijn van een authentieke gegevensbron.

[11] Zie overwegingen nrs. 69 en volgende.

17. Ten tweede, **indien *uiteindelijk,* als onderdeel van het standaardiseringsproces, toch zou worden besloten om het begrip van authentieke gegevensbron te wijzigen als** gevolg van de hervorming van de eIDAS-verordening, wil de Autoriteit de aanvrager wijzen op de volgende twee punten met betrekking tot het Wetsontwerp zoals het nu is geformuleerd.

18. Allereerst **moet in de memorie van toelichting worden gerechtvaardigd waarom het Belgisch federaalrechtelijke begrip authentieke gegevensbron volledig in overeenstemming moet worden gebracht met het begrip** dat zal worden vastgelegd in de hervorming van de **eIDAS-verordening**. Deze analyse moet worden opgenomen in de **effectbeoordeling** inzake gegevensbescherming die gezien de reikwijdte van het Wetsontwerp moet worden uitgevoerd.

19. Dit zou inhouden dat moet worden vastgesteld of de doelstelling(en) (functies) van het begrip authentieke bron in de eIDAS-verordening identiek zijn aan de doelstelling(en) (functies) van het begrip in het Belgisch recht en dat bijgevolg een begrip dat specifiek is voor het Belgische recht niet langer nodig zou zijn. **In dat geval zou het passend zijn om expliciet te verwijzen naar de definitie in de eIDAS-verordening**.

20. Omgekeerd, als het Europese begrip niet zou kunnen volstaan om de doelstellingen van Belgisch recht bereiken, zou het dispositief van het Wetsontwerp dan twee definities moeten bevatten, overeenkomstig de relevante doelstellingen die worden nagestreefd door de wet van 2012 en die welke worden nagestreefd door de eIDAS-verordening, zodat de reikwijdte van de verschillende begrippen duidelijk blijkt uit het Wetsontwerp.

21. **Het is aan de aanvrager om deze analyse te motiveren op basis van de uiteindelijke en definitieve bepalingen van de hervormde eIDAS-verordening**. In dit verband vestigt de Autoriteit ook de aandacht van de aanvrager op het feit dat een authentieke bron ook kenmerken met betrekking tot goederen kan omvatten (mogelijk opgenomen in het begrip "*goederen*" onder de hervormde eIDAS-verordening). De huidige definitie van het Wetsontwerp heeft alleen betrekking op kenmerken met betrekking tot natuurlijke of rechtspersonen[12] .

22. Verder benadrukt de Autoriteit dat overeenkomstig de beginselen van voorzienbaarheid en rechtmatigheid die zijn vastgelegd in artikel 8 EVRM, artikel 22 van de Grondwet, artikel 8 van het Handvest van de grondrechten van de Europese Unie en artikel 6, lid 3, van de AVG, **"*bestuurlijk handelen*" niet voldoende is om een gegevensbron als authentiek te erkennen in het kader van het Wetsontwerp,** gezien de juridische gevolgen hiervan in termen van de verwerking van

[12] Maar de aanvrager heeft bevestigd dat hij zich zal moeten aanpassen aan de laatste versie van het Europese concept.

persoonsgegevens. **In de overwegingen 4-6[13] en 35-3 7[14] van haar advies nr. 143/2023 heeft de Autoriteit herhaald dat de beginselen van voorzienbaarheid en rechtmatigheid van toepassing zijn op de uitwisseling van gegevens uit authentieke bronnen en verwijst zij naar deze ontwikkelingen**.

### II.2.2. Aanwijzing en criteria voor de aanwijzing van authentieke bronnen

23. In lijn met het voorgaande commentaar **wijzigt het Wetsontwerp het beginsel dat thans is vastgelegd in artikel 27, § 2, van de wet van 2012, volgens hetwelk,** op voorstel van het

---

[13] Met weglating van de verwijzingen luiden deze overwegingen als volgt (onderstreept en vetgedrukt in de oorspronkelijke tekst) :

*" **De Autoriteit heeft** in de **overwegingen 5 tot en met 19 van haar vorige advies reeds** uitvoerig **haar standpunt uiteengezet over de toepassing van de beginselen van voorspelbaarheid en rechtmatigheid, zoals vastgelegd in de artikelen 8 EVRM en 22 van de Grondwet,** in de context van de samenwerkingsovereenkomst inzake gegevensuitwisseling en het hergebruik van gegevens uit authentieke bronnen, gezien de specifieke aard van het gebied waarop deze overeenkomst betrekking heeft en de voorziene regelingen. De Autoriteit **verwijst in eerste instantie naar deze overwegingen**.*

*Met name in overweging 7 van haar vorige advies wijst de Autoriteit erop dat de beginselen van voorzienbaarheid en rechtmatigheid* "moeten worden toegepast met inachtneming van de algemene en abstracte aard van het ontwerp, dat in wezen een kader vaststelt voor de uitwisseling in Wallonië tussen overheidsinstanties van gegevens uit authentieke gegevensbronnen door een enkele verzameling bij burgers en bedrijven mogelijk te maken, en voor de controle op de gegevensverwerking door deze instanties, zonder rechtstreeks te voorzien in specifieke gegevensverwerking (zij het met enkele nuances, zie [...]). Naast dit algemene doel bepaalt het ontwerp zelf dus niet voor welke specifieke en expliciete doeleinden gegevens uit authentieke bronnen mogen worden verwerkt. [...] ".

*Met andere woorden, in concrete termen, de **conformiteit van de gegevensverwerking die wordt uitgevoerd in het kader van het Wetsontwerp met de beginselen van voorzienbaarheid en rechtmatigheid zal in concreto en systematisch moeten worden beoordeeld aan de hand van drie regelgevende kaders**: dat van de authentieke gegevensbron, dat van het Wetsontwerp en dat van de activiteit van de deelnemende overheidsdienst die van plan is de gegevens van de authentieke bron in kwestie te verwerken. In het bijzonder volgt artikel 7, § 2, al. 2 van het Wetsontwerp deze logica wanneer het stelt:* "Het gebruik van de diensten van de KBO [··· ] verleent de deelnemende overheidsdiensten niet het recht op toegang tot gegevens waartoe zij geen toegang zouden hebben door rechtstreeks de authentieke gegevensbronnen te raadplegen".

[14] Zonder de verwijzingen luiden deze overwegingen als volgt (vet en onderstreept in de oorspronkelijke tekst):

*"De Autoriteit merkt op dat de uitwisseling van persoonsgegevens nog steeds een regelgevend kader vereist dat voldoet aan de hierboven genoemde beginselen van voorzienbaarheid en rechtmatigheid. In feite is het hele Wetsontwerp gericht op het bieden van een kader (zij het een logisch en onvolledig kader, zoals is opgemerkt) voor de uitwisseling van gegevens uit authentieke bronnen. Het feit dat gegevens al kunnen worden uitgewisseld tussen overheidsinstanties zonder dat een database als authentieke gegevensbron wordt aangemerkt, is irrelevant voor de analyse.*

***De Autoriteit is van mening dat het Wetsontwerp ten minste moet bepalen dat een overheidsbesluit moet worden vastgesteld om een gegevensbank als authentieke gegevensbron te kwalificeren**. De status van authentieke bron die aan een gegevensbank wordt toegekend, vormt immers duidelijk een essentieel element van de uitgevoerde gegevensverwerking (het houdt verband met het doel van de verwerking): het is uit deze status dat de indirecte (en verplichte) methode van gegevensverzameling bij de betrokken bron, via de KBO, in het kader van de uitvoering van het Wetsontwerp, voortvloeit. Het is daarom alleen in het licht van de specifieke kenmerken van het Wetsontwerp en de beweegreden ervan (d.w.z. de invoering van een algemeen dispositief dat het systematische gebruik van authentieke gegevensbronnen organiseert) dat de Autoriteit eerder heeft aanvaard dat de status van authentieke bron kon worden toegekend door een regelgevende norm (en niet rechtstreeks door een norm van de rang van wet), zonder daarbij de beginselen van voorzienbaarheid en rechtmatigheid te miskennen die zijn vastgelegd in artikel 8 EVRM en artikel 22 van de Grondwet [...]. Door deze bevoegdheid te delegeren aan een overheidsinstantie zoals het KBO (in concreto, aan de verantwoordelijke) worden deze beginselen niet geëerbiedigd.*

*Met betrekking tot de voorwaarden waaraan een databank moet voldoen om als authentieke gegevensbron te worden aangewezen, bepaalt artikel 5, § 1 , lid 3, van het Wetsontwerp dat* "de databank gebaseerd moet zijn op een norm met juridische waarde" (onderstreping toegevoegd door de Autoriteit). *De Autoriteit is van mening dat de uitdrukking "van juridische waarde" dubbelzinnig is en moet worden vervangen door "decreet". Gezien de hierboven genoemde beginselen van voorzienbaarheid en rechtmatigheid **moeten de essentiële elementen van gegevensverwerking via een databank die een authentieke gegevensbron vormt, worden gedefinieerd in een norm met de status van wet**[···] . In dit opzicht kunnen alleen gegevensbanken waarvan de essentiële elementen zijn vastgelegd in een verordening met de status van wet, worden geïdentificeerd als een authentieke bron. In het **geval van de Waalse en Franse communautaire rechtsordes moet dus** worden **verwezen naar het decreet**. Artikel 5, § 1 , lid 3, van het Wetsontwerp moet dus dienovereenkomstig worden aangepast* ".

Coördinatiecomité[15] **, de Koning bij besluit vastgesteld in de ministerraad, enerzijds** de criteria **bepaalt** op basis waarvan gegevens als authentiek worden aangemerkt (criteria die nu rechtstreeks worden overgenomen door het Wetsontwerp, in het dispositief van de wet van 2012), en anderzijds **welke gegevens als authentiek kunnen worden aangemerkt**. Het Wetsontwerp voorziet nu in het volgende:

> *"Het coördinatiecomité merkt de gegevens aan als authentiek indien ze voldoen aan de volgende criteria :*
>
> *1. de registratie van gegevens en de verstrekking ervan komen voort uit taken die bij of krachtens een wet, decreet of bevel zijn opgedragen ;*
>
> *2. de gebruiker bedoeld in artikel 2, lid 10, a) tot g), die verantwoordelijk is voor het verzamelen of beheren van de gegevens, voorziet in en voldoet aan procedures die waarborgen dat de gegevens te allen tijde juist, volledig, veilig, leesbaar en beschikbaar zijn, en stelt het Coördinatiecomité periodiek op de hoogte*".

24. Het commentaar bij het eerste criterium luidt als volgt:

> *"Een eerste criterium om gegevens als authentiek aan te merken is dat de registratie van deze gegevens moet zijn voorgeschreven bij of krachtens een wet, decreet of ordonnantie. Dit eerste criterium is vooral belangrijk voor gegevens die worden verzameld door organisaties buiten de publieke sector. Deze organisaties - bijvoorbeeld beroepsverenigingen van bepaalde vrije beroepen - verzamelen ook gegevens waarvan de registratie niet wordt opgelegd door een wettelijke of reglementaire bepaling. Dergelijke gegevens, waarover de overheidsinstanties geen controle kunnen uitoefenen, kunnen nooit als authentieke gegevens worden aangemerkt. Indien ze toch als zodanig worden aangemerkt, zullen de overheidsinstanties praktisch verplicht zijn om met deze gegevens te werken alsof ze deze zelf hebben verzameld. Gegevens die worden geregistreerd en beheerd door organisaties buiten de publieke sector kunnen daarom worden aangemerkt als authentieke gegevens, op voorwaarde dat de registratie ook voortvloeit uit een wettelijke of reglementaire eis.*
>
> *Dit criterium houdt niet in dat de gegevens uitdrukkelijk moeten worden opgesomd in een wet, Koninklijk Besluit, decreet of ordonnantie, maar veeleer dat de registratie van de gegevens moet voortvloeien uit de taken die worden opgelegd bij of krachtens de wet aan de organisatie die de gegevens registreert*" (onderstreping toegevoegd door de Autoriteit).

[15] Het Coördinatiecomité is, afhankelijk van het Wetsontwerp, samengesteld uit de verantwoordelijke van elke gebruiker bedoeld in artikel 2, lid 10, a) tot g), de verantwoordelijke van elke dienstenintegrator, in de zin van artikel 2, lid 1, en de voorzitter van het Directiecomité van de Federale Overheidsdienst Strategie en Ondersteuning.

25. De Autoriteit heeft de aanvrager ondervraagd over de reden voor het schrappen van de rol van de Koning (via een decreet waarover de ministerraad had beraadslaagd). De aanvrager antwoordde als volgt:

> *"Het lijkt ons opportuun om de voorwaarden expliciet op te nemen in de wet om een grotere juridische zekerheid te bieden aan de betrokken organisaties.* ***Het Coördinatiecomité is zeker het best geplaatst om hierover te beslissen, aangezien het over de nodige expertise beschikt****. In dit verband moet worden verwezen naar zijn handleiding betreffende de totstandbrenging van een authentieke bron.*
> *(Cfr.* https://bosa.*belgium.be/sites/default/files/documents/bosa_dt_guide_pratique_-_mise_en_place_dune_source_authentique_v1.0.pdf, gepubliceerd op de volgende webpagina: https://bosa.belgium.be/fr/themes/administration-numerique/composants-et-plateformes-numeriques/sources-authentiques)*
> *Dit comité geeft ook advies aan de betrokken organisaties over hoe ze aan de voorwaarden moeten voldoen. Naar onze mening heeft* ***het geen toegevoegde waarde om dit door een Koninklijk Besluit te laten bekrachtigen***" (vetgedrukt toegevoegd door de Autoriteit).

26. Eerst en vooral is **de Autoriteit Persoonsgegevens van mening dat de identificatie van de criteria voor de aanwijzing van een authentieke bron in de wet van 2012 zelf een positieve bijdrage van het Wetsontwerp is op het gebied van de bescherming** van **persoonsgegevens.** Op deze manier zorgt het Wetsontwerp ervoor dat een parlementair debat over het onderwerp kan plaatsvinden en garandeert het meer juridische stabiliteit.

27. In dit verband verwijst de Autoriteit naar **de overwegingen 4-6 en 35-36 van haar advies nr. 143/2023**[16] . **De noodzaak van een Koninklijk Besluit (in dit geval besproken in de ministerraad) om de authentieke gegevens (of bronnen) te identificeren is gerechtvaardigd in het licht van de beginselen van voorzienbaarheid en rechtmatigheid**: een dergelijk besluit vormt een **normatieve handeling** die in dit geval, gezien de eerdere adviespraktijk van de Autoriteit, kan bijdragen aan de bepaling van essentiële elementen van de betrokken gegevensverwerkingen door de relevante authentieke bronnen (of gegevens) in kwestie aan te wijzen[17] . Een kwalificatie door het Coördinatiecomité vormt geen norm en voldoet niet aan de eisen van voorzienbaarheid en rechtmatigheid. **De Autoriteit is van mening dat het Wetsontwerp op dit punt moet worden aangepast**.

[16] Zie voetnoten 13-14.

[17] Zo heeft de Autoriteit in het verleden aanvaard dat de loutere aanduiding van de authentieke bron kan gebeuren door een reglementaire maatregel (een decreet van de Waalse regering in het betrokken advies), op voorwaarde dat de rest van de essentiële elementen van de beoogde verwerking zijn vastgelegd in een norm van rechtsvorm.

28. Bovendien, en zoals de Autoriteit heeft benadrukt in het kader van haar eerder genoemde advies[18], met betrekking tot het eerste criterium voor het aanwijzen van een authentieke bron krachtens het Wetsontwerp (wettelijke taak), vereist de toepassing van de beginselen van voorzienbaarheid en rechtmatigheid **dat de taak (of verplichting) van de overheidsinstantie (of private entiteit)** op grond waarvan de betreffende authentieke gegevens worden verzameld of gecreëerd[19]**, moet worden vastgelegd in een rechtsnorm, evenals de essentiële elementen van de verwerking van die gegevens door de betrokken overheidsinstantie**. De Autoriteit is daarom van mening dat het Wetsontwerp (dispositief en memorie van toelichting) op dit punt **moet worden aangepast** en dat er geen rechtvaardiging is voor het schrappen van de noodzaak van een in de ministerraad overlegd Koninklijk Besluit, zoals momenteel voorzien in de wet van 2012.

29. Vervolgens, **wat betreft de criteria voor de aanwijzing van een authentieke gegevensbron,** heeft de Autoriteit haar standpunten al uiteengezet in overweging 64 van haar advies 154/2023 en de overwegingen 38-39 van haar advies 143/2023. Het eerste criterium zoals voorzien in het Wetsontwerp stelt dat "*de registratie en verstrekking van gegevens*" moet voortvloeien uit de betreffende wettelijke taken.

30. In dit verband vestigt de Autoriteit, in plaats van op "*registratie*", de aandacht van de aanvrager op het feit dat het **verzamelen of creëren van de gegevens** in principe moet voortvloeien uit een (wettelijke) opdracht van de betreffende bron. **De doorslaggevende factor is** dus **dat de betrokken entiteit, gezien haar wettelijke taken met betrekking tot de betreffende gegevens, en met name het verzamelen/creëren en bijwerken ervan, in de beste positie verkeert om de kwaliteit ervan te waarborgen en deze te communiceren[20] aan andere entiteiten voor de doeleinden die zij nastreven**.

31. **Het** is echter niet **uitgesloten** dat **registratie van de gegevens** in bepaalde gevallen **bepalend kan zijn** wanneer, gelet op het doel van de bij wet voorziene verwerking, een specifieke en gerechtvaardigde behoefte aan gecentraliseerde opslag (integratie van gegevens met het oog op het creëren van een authentieke bron) noodzakelijk is, zoals wordt geïllustreerd door het voorbeeld van

[18] In het bijzonder en reeds in overweging 19 van haar advies nr. 65/2019 van 27 februari 2019 *betreffende een ontwerp van samenwerkingsovereenkomst tot wijziging van de samenwerkingsovereenkomst van 23 mei 2013 tussen het Waals Gewest en de Franse Gemeenschap met betrekking tot de ontwikkeling van een gezamenlijk initiatief voor gegevensuitwisseling en het gezamenlijk beheer van dat initiatief (CO-A-2019-014 + CO-A-2019-044), heeft* de Autoriteit eraan herinnerd dat de authentieke gegevensbron *mutatis mutandis* moet worden gecreëerd en georganiseerd door een norm van de rang van het recht.

[19] Zie overweging 22.

[20] Op dit punt verwelkomt de Autoriteit het feit dat het eerste criterium van het Wetsontwerp ook betrekking heeft op de communicatie van gegevens.

het Rijksregister[21] . De Autoriteit is van mening dat **de aanvrager** op dit punt **het dispositief van het Wetsontwerp moet verduidelijken**.

32. Wat het tweede criterium betreft, "*de gebruiker bedoeld in artikel 2, lid 10, onder a) tot en met g), die belast is met het verzamelen of beheren van de gegevens, voorziet en respecteert procedures die ervoor zorgen dat de gegevens te allen tijde nauwkeurig, volledig, veilig, leesbaar en beschikbaar zijn, en stelt hij het Coördinatiecomité daarvan periodiek in kennis*". De Autoriteit is van mening **dat ook moet** worden **verwezen naar het normatieve kader dat op de betrokken gebruiker van toepassing is**. **Met het oog op de nagestreefde doelstellingen dient dit normatieve kader bepalingen te bevatten met betrekking tot de kwaliteit van gegevens, hun bijwerking** (identificatie van gebeurtenissen die leiden tot bijwerken/wijzigen van gegevens, eventuele frequentie, enz.

**II.3. Deelnemende overheidsdiensten en gebruikers**

33. Het begrip "*deelnemende overheidsdienst*" uit artikel 2, lid 10, van de wet van 2012 is vervangen door het begrip "*gebruiker*". In de memorie van toelichting wordt dit als volgt uitgelegd:

> *"De term "deelnemende overheidsdienst" is vervangen door de term "gebruiker" omdat overheidsdiensten niet de enigen zijn die gegevens ter beschikking kunnen stellen via de federale dienstenintegrator. Overeenkomstig artikel 46 van de wet kunnen ook andere organisaties worden aangewezen. Bovendien zijn de ontvangers van de gegevens zowel de overheidsdiensten als andere rechthebbenden zoals burgers en bedrijven en hun vertegenwoordigers.*
>
> *De term "gebruiker" is duidelijker gedefinieerd en er is toegevoegd dat de gegevens die door de federale dienstenintegrator ter beschikking worden gesteld, beschikbaar zijn voor rechthebbenden op die gegevens. Dit kunnen rechthebbenden zijn van een aangewezen authentieke bron zoals bepaald in de wetgeving over de bron en aan wie de gegevens moeten worden verstrekt. Het kan de betrokkene zijn die het recht heeft te weten welke gegevens over hem of haar worden verwerkt. Het kan de houder van een Europese portemonnee voor digitale identiteit zijn die gegevens van overheidsinstanties kan ontvangen om deze aan derden aan te bieden. Het kan gaan om degenen die recht hebben op informatie met het oog op hergebruik, organisaties die recht hebben op openbare gegevens, zowel in België als in het buitenland, volgens de DGA.*

[21] Zie bijvoorbeeld de wet van 8 augustus 1983 *tot instelling van een Rijksregister van natuurlijke personen* (en artikel 4 daarvan).

*Het Vast Comité van Toezicht op de politiediensten, het Vast Comité van Toezicht op de inlichtingendiensten en het Coördinatieorgaan voor de dreigingsanalyse worden toegevoegd als gebruikers. Zij moeten de beschikbaar gestelde gegevens kunnen gebruiken voor de uitvoering van hun taken.*

*Het Informatieveiligheidscomité wordt toegevoegd. Dit comité is bevoegd met betrekking tot de communicatie van persoonsgegevens" (onderstreping toegevoegd door de Autoriteit).*

34. Het Wetsontwerp voegt verschillende organisaties toe aan het begrip gebruiker, waaronder :

- Het *Vast Comité van Toezicht op de politiediensten*;
- Het *Vast Comité van Toezicht op de inlichtingendiensten*;
- Het *Coördinatieorgaan voor de dreigingsanalyse*;
- Het *Informatieveiligheidscomité* ;
- De geïntegreerde politie, diensten die onder Defensie vallen (het ministerie van Defensie valt al onder de wet van 2012);
- De rechterlijke macht, met inbegrip van de diensten voor bijstand aan haar leden, de publiekrechtelijke rechtspersonen bedoeld in artikel 1, lid 3, van de wet van 22 juli 1993 *houdende bepaalde maatregelen inzake ambtenarenzaken*[22] ;

[22] Of :
*"de Regie der Gebouwen;*
*- het Federaal Agentschap voor de Veiligheid van de Voedselketen;*
*- het Belgisch Interventie- en Restitutiebureau;*
*- (...); <L 2003-04-03/68, art. 33, 016;* ***In werking :*** *01-12-2006>*
*- de Centrale Dienst voor Sociale en Culturele Actie van het Ministerie van Landsverdediging;*
*- het Nationaal Geografisch Instituut;*
*- [2 het War Heritage Instituut]2;*
*- de Controledienst voor de ziekenfondsen en de landsbonden van ziekenfondsen;*
*- de Controledienst voor de Verzekeringen;*
*- [1 ...]1;*
*- het Fonds voor Arbeidsongevallen;*
*- het Fonds voor Beroepsziekten;*
*- [2 ...]2;*
*- de Hulpkas voor ziekte- en invaliditeitsverzekering;*
*- de Hulpkas voor werkloosheidsuitkeringen;*
*- [1 ...]1;*
*- de Rijksdienst voor Kinderbijslag voor Werknemers;*

- Natuurlijke personen of rechtspersonen aan wie bij wet taken van openbare dienst of taken van algemeen belang zijn toegekend en die niet onder de wet van 21 maart 1991 *betreffende de hervorming van sommige economische overheidsbedrijven vallen*;

- Elke persoon en instantie aangewezen door de Koning overeenkomstig artikel 46[23] , voor zover deze een of meer authentieke bronnen of gegevensbanken ter beschikking stelt of gegevens opvraagt via de federale dienstenintegrator;

- En elke persoon en autoriteit die, volgens de federale of Europese regelgeving en volgens de voorwaarden die verbonden zijn aan de gegevens uit authentieke bronnen of gegevensbronnen van gebruikers zoals bedoeld in artikel 2, lid 10, a tot g, gemachtigd is om deze gegevens te raadplegen of te ontvangen.

35. Zoals gewijzigd, omvat artikel 2, lid 10, van de wet van 2012, ook nog steeds een uitzondering die van toepassing is op de federale dienstenintegrator zelf en een reeks organisaties die verband houden met de sociale zekerheid. Op dit punt nodigt de Autoriteit de aanvrager uit om **zijn verwijzing naar artikel 1, lid 3, van de wet van 22 juli 1993 *betreffende bepaalde maatregelen inzake openbare diensten* te wijzigen met inachtneming van deze uitzondering**.

---

*- de Nationale Dienst voor Sociale Zekerheid;*

*- [1 ...]1;*

*- het Rijksinstituut voor de Sociale Verzekeringen der Zelfstandigen;*

*- het Rijksinstituut voor Ziekte- en Invaliditeitsverzekering;*

*- de Rijksdienst voor Jaarlijkse Vakantie;*

*- de Rijksdienst voor Arbeidsvoorziening;*

*- [5 de Federale Pensioendienst;]5*

*- de Kruispuntbank van de Sociale Zekerheid;*

*- (Het Federaal Planbureau;) <L 2004-12-27/30, art. 506, 017;* ***In werking :*** *10-01-2005>*

*(- Instituut voor de gelijkheid van vrouwen en mannen) <L 2003-02-27/50, art. 2, 015;* ***In werking:*** *03-04-2003>.*

*- [5 ...]5;*

*(- Agentschap voor de oproepen tot de hulpdiensten;) <L 2006-07-20/39, art. 75, 019;* ***In werking:*** *07-08-2006>*

*(Federaal Agentschap voor Geneesmiddelen en Gezondheidsproducten;) <L 2006-07-20/78, art. 16, 020;* ***In werking:*** *01-01-2007>*

*[2 - het platform eHealth;]2* ".

[23] Artikel 46 van de wet van 2012 luidt als volgt:

*" Onder de voorwaarden en volgens de modaliteiten die Hij bepaalt, kan de Koning, bij besluit genomen in de ministerraad op voorstel van het overlegcomité van dienstenintegratoren en na advies van de Commissie voor de Bescherming van Persoonlijke Levenssfeer, de rechten en verplichtingen voortvloeiend uit deze wet en de uitvoeringsmaatregelen ervan uitbreiden naar andere personen of organisaties dan de deelnemende overheidsdiensten. Een dergelijke uitbreiding van rechten en verplichtingen mag niet betrekking hebben op taken die vallen onder het werkterrein van een andere dienstenintegrator* ".

36. Onder deze omstandigheden, **afgezien van enkele verduidelijkingen in de memorie van toelichting[24], is het niet langer mogelijk om concreet vast te stellen wie de potentiële gebruikers zijn in de zin van de wet van 2012**. De Autoriteit heeft de aanvrager ondervraagd over de motivatie en de praktische redenen die hebben geleid tot een dergelijke uitbreiding van het begrip "deelnemende openbare dienst", buiten wat is gespecificeerd in de memorie van toelichting. Zij verzocht de aanvrager ook te verduidelijken wie de andere personen zijn die worden bedoeld in artikel 46 van de wet van 2012, evenals welke privépersonen mogelijk authentieke bronnen beschikbaar zouden kunnen stellen. De Autoriteit was ook niet langer zeker van het belang van artikel 46 van de wet van 2012. Zij heeft de aanvrager hierover ondervraagd, en deze verduidelijkt als volgt:

> *"De uitbreiding van gebruikers betreft de personen en entiteiten die gegevens kunnen raadplegen of ontvangen via de federale dienstenintegrator.*
> *Het blijft belangrijk om op basis van artikel 46 te voorzien in de mogelijkheid* ***om de categorie van entiteiten die gegevens mogen verstrekken via de federale dienstenintegrator uit te breiden (bijvoorbeeld de federatie van notarissen, de Nationale kamer van gerechtsdeurwaarders, de orde van advocaten, het ITAA - Instituut van Belasting- en Boekhoudingsadviseurs,*** *enz.)*
>
> *Als voorbeeld van een reden* ***om de categorie ontvangers uit te breiden kan worden vermeld*** *FOD Mobiliteit, dat overeenkomstig zijn eigen wetgeving* ***gegevens*** *mag verstrekken* ***aan private entiteiten*** *(d.w.z. andere dan deelnemende overheidsdiensten), wat niet is voorzien in de huidige bepalingen van de wet van 2012.*
>
> *De wijziging van de categorie gebruikers heeft tot doel de* ***potentiële categorieën ontvangers waarvoor de gegevens toegankelijk zijn*** *uit te breiden. Terwijl voorheen* ***de toegang alleen betrekking had op communicatie tussen deelnemende overheidsdiensten****, heeft de uitbreiding betrekking op communicatie van de betrokken gebruikers naar alle partijen die gemachtigd zijn om deze gegevens van deze gebruikers te ontvangen. Dit is* ***nodig om te voldoen aan verschillende verplichtingen en behoeften in het kader van de toepassing van de Digital Governance Act, de Single Digital Gateway en de*** *gewijzigde* ***eIDAS*** *(de digitale portemonnee), waarvoor de federale*

[24] De enige concrete verduidelijking betreft het feit dat gebruikers rechthebbenden zijn op de betreffende gegevens:
"
*De term "gebruiker" is duidelijker gedefinieerd en er is toegevoegd dat de gegevens die door de federale dienstenintegrator ter beschikking worden gesteld, beschikbaar zijn voor alle rechthebbenden op die gegevens. Dit kunnen rechthebbenden zijn van een aangewezen authentieke bron zoals bepaald in de wetgeving over de bron en aan wie de gegevens moeten worden verstrekt. Het kan de betrokkene zijn die het recht heeft te weten welke gegevens over hem of haar worden verwerkt. Het kan de houder van een Europese portemonnee voor digitale identiteit zijn die gegevens van overheidsinstanties kan ontvangen om deze aan derden aan te bieden. Het kan gaan om degenen die recht hebben op informatie met het oog op hergebruik, organisaties die recht hebben op openbare gegevens, zowel in België als in het buitenland, volgens de DGA*." (onderstreept door de Autoriteit).

*dienstenintegrator nu zal optreden om gegevens ter beschikking te stellen aan rechthebbenden (personen en entiteiten)*" (vetgedrukt door de Autoriteit).

Ten tweede heeft de aanvrager met betrekking tot deze verschillende verplichtingen de volgende bijzonderheden verstrekt:

*"Single digital gateway*

- *Verordening (EU) 2018/1724 van het Europees Parlement en de Raad van 2 oktober 2018 tot oprichting van één digitale toegangspoort voor informatie, procedures en diensten voor ondersteuning en probleemoplossing en houdende wijziging van Verordening (EU) nr. 1024/2012, art. 6 en art. 14.*
- *UITVOERINGSVERORDENING (EU) 2022/1463 VAN DE COMMISSIE van 5 augustus 2022 tot vaststelling van technische en operationele specificaties van het technisch systeem voor de grensoverschrijdende geautomatiseerde uitwisseling van bewijs en de toepassing van het eenmaligheidsbeginsel overeenkomstig Verordening (EU) 2018/1724 van het Europees Parlement en de Raad, art. 1 tot en met 36*
- *SPF BOSA is verantwoordelijk voor de ontwikkeling en de terbeschikkingstelling van het Only Once Technical System in België, in samenwerking met de gegevensverstrekkers in België, de andere. De toewijzing van deze taak is voorzien in (het ontwerp van) het samenwerkingsakkoord tussen de federale overheid en de deelentiteiten.*

*Date Governance act*

- *het vervullen van de rollen van centraal informatiepunt en van bevoegd orgaan voor de technische bijstand zoals bedoeld respectievelijk in de artikelen 8 en 7, lid 1 van de Europese Verordening (EU) 2022/868 van het Europees Parlement en de Raad van 30 mei 2022 betreffende Europese datagovernance en tot wijziging van Verordening (EU) 2018/1724*

*eIDAS-wet (wijziging)*

- *in het ontwerp van wijziging van eIDAS Act wordt voorzien dat elke lidstaat een Europese portemonnee voor digitale identiteit moet aanbieden. In België zal FOD BOSA instaan voor de ontwikkeling en ter beschikking stelling van die Europese portemonnee voor digitale identiteit. Het ontwerp van wijziging van eIDAS werd nog niet goedgekeurd dus er kan in de wettekst nog niet naar verwezen worden.*

  *Conform de definitie zoals voorzien in de het ontwerp van de wijziging van de eIDAS-wet is de Europese portemonnee voor digitale identiteit een elektronisch identificatiemiddel dat de gebruiker in staat stelt om persoonlijke identificatiegegevens en elektronische attesten van kenmerken veilig op te slaan, te beheren en te valideren om ze te verstrekken aan gebruikerspartijen en andere gebruikers van Europese portemonnees voor digitale*

*identiteiten, en om te ondertekenen met gekwalificeerde elektronische handtekeningen of om stempels aan te brengen met gekwalificeerde elektronische stempels*".

37. De Autoriteit neemt nota van deze toelichtingen. Zij vestigt echter de aandacht van de aanvrager op het feit dat **artikel 2, lid 10, onder h) en g),** van de wet van 2012, zoals gewijzigd bij het Wetsontwerp, **elkaar gedeeltelijk lijken te overlappen**. Onder g), dat verwijst naar artikel 46 van het Wetsontwerp, valt immers ook elke persoon of autoriteit aangewezen door de Koning die gegevens "*terugkrijgt*" via de federale dienstenintegrator. Punt h) is echter al zeer breed gericht op de ontvangers van de gegevens die beschikbaar zijn via de integrator.

38. **Meer in het algemeen lijkt f), dat zeer breed geformuleerd is, ook entiteiten te kunnen omvatten die door de aanvrager worden genoemd om de reikwijdte van artikel 46 te illustreren.** Zijn bijvoorbeeld "*de federatie van notarissen, de Nationale kamer van gerechtsdeurwaarders, de orde van advocaten, het ITAA - Instituut van Belasting- en Boekhoudingsadviseurs*" niet reeds entiteiten die door de geldende wetgeving zijn belast met bepaalde taken van openbaar belang of op zijn minst met specifieke wettelijke verplichtingen met betrekking tot de gegevens die zij verzamelen en die relevant kunnen zijn voor de uitvoering van de wet van 2012?

39. Bovendien **is artikel 46 van de wet van 2012 niet beperkt tot entiteiten die gegevens "*verstrekken*" via de federale dienstenintegrator**. Breder gezien, en zoals gewijzigd door het Wetsontwerp, geeft het in feite de bevoegdheid om "*alle of sommige van de rechten en verplichtingen die voortvloeien*" *uit* de wet van 2012 uit te breiden naar "*andere personen of instanties dan de gebruikers bedoeld in artikel 2, lid 10, a) tot f), en h)*".

40. Onder deze omstandigheden is de Autoriteit van mening dat de aanvrager **het dispositief van het Wetsontwerp moet verduidelijken en de artikelen 2, 10 en 46 van de wet van 2012 zodanig moet wijzigen dat deze de gecommuniceerde bedoelingen correct weergeven**, namelijk om, via artikel 46 van het Wetsontwerp, toe te staan dat andere entiteiten dan de overheidsinstanties die momenteel onder het Wetsontwerp vallen gegevens kunnen verstrekken via de federale dienstenintegrator, wanneer zij belast zijn met een wettelijke verplichting of een taak van openbaar belang die het verzamelen (of creëren) van de betreffen gegevens vereist. **Het Wetsontwerp moet de verschillende betrokken entiteiten duidelijk identificeren en afbakenen**: ontvangers van gegevens (de breedste categorie), openbare entiteiten (volgens de memorie van toelichting gaat het om "overheidsdiensten") en privé-entiteiten die belast zijn met specifieke taken van openbaar belang (of wettelijke verplichtingen).

41. Bovendien is de Autoriteit van mening dat artikel 46 van de wet van 2012, inclusief zoals gewijzigd bij het Wetsontwerp, **problematisch** is met **betrekking tot de beginselen van voorzienbaarheid**

**en rechtmatigheid die eerder zijn benadrukt**[25] , aangezien het de Koning toestaat de rechten en verplichtingen waarin de wet van 2012 voorziet, te moduleren afhankelijk van de instanties aan wie hij de toepassing van het dispositief in het Wetsontwerp zou uitbreiden. Opnieuw is de Autoriteit van mening dat de bepaling **moet worden geherformuleerd in het licht van de intenties van de aanvrager (door de uitbreiding te beperken tot de mededeling van gegevens, zoals hierboven vermeld),** vooral omdat het toepassingsgebied van de wet van 2012, zoals gewijzigd bij het Wetsontwerp nu is uitgebreid (de dienstenintegrator heeft bijvoorbeeld nieuwe taken gekregen): **de wet van 2012 breidt zich nu verder uit dan de uitwisseling van gegevens tussen overheidsinstanties**.

42. Bovendien wijst de Autoriteit erop dat het beginsel om een beroep te doen op de federale dienstenintegrator in principe niet **bindend is**[26] . Bijgevolg **zou** de uitbreiding van de toepassing van de wet van 2012 tot private entiteiten **ook een mogelijkheid moeten zijn voor deze entiteiten**, net zoals voor de gebruikers bedoeld in artikel 2, lid 10, a) tot g), van de wet van 2012 zoals gewijzigd door het Wetsontwerp. **Bij gebrek hieraan zou** het **verschil in behandeling** door de aanvrager moeten worden **gerechtvaardigd** in het kader van het gelijkheidsbeginsel, een vraag waarover de Raad van State zich dan moet uitspreken.

## II.3 Taken van de dienstenintegrator

### II.3.1. Gegevensuitwisseling, gegevensattestatie en portemonnee van digitale identiteit

43. Artikel 4, lid 1, van de wet van 2012, zoals gewijzigd bij het Wetsontwerp, voorziet dat de dienstenintegrator "*de in een of meer gegevensbanken opgeslagen gegevens ontvangt, tijdelijk bewaart gedurende de tijd die nodig is om het beoogde doel te bereiken, en voldoet aan verzoeken tot raadpleging en mededeling van die gegevens of overgaat tot de geïntegreerde mededeling en attestering van die gegevens*" (onderstreept door de Autoriteit). De bewaring wordt ook behandeld in artikel 4, lid 8, van de wet van 2012 zoals gewijzigd bij het Wetsontwerp.

44. In het Wetsontwerp worden begrippen gebruikt die nog niet bestaan in het positief recht, zoals "*portemonnee voor digitale identiteit*" en "*gegevensattesten*". Zo voorziet artikel 4 van de wet van 2012, zoals gewijzigd bij het Wetsontwerp, dat de dienstenintegrator gegevens meedeelt "*die in een of meer gegevensbanken zijn opgeslagen of geïntegreerde mededeling en attestering van dergelijke gegevens uitvoert*"[27] . Artikel 12, § 1, van de wet van 2012, zoals gewijzigd bij het Wetsontwerp,

[25] Zie overweging 22.

[26] Zie overwegingen 69 en volgende.

[27] Artikel 4, lid 1, van de wet van 2012 zoals gewijzigd door het Wetsontwerp.

behandelt de bewijskracht van gegevensattesten, en lid 2 van dat artikel behandelt de gelijkschakeling van papieren documenten met digitale attesten.

45. De dienstenintegrator "*ontwikkelt de technische modaliteiten en voorwaarden om de toegangskanalen, waaronder webdiensten, mobiele applicaties, portemonnee voor digitale identiteit en online portalen, op de meest efficiënte en veilige manier te ontwikkelen en te verbinden*"[28] .

46. Met betrekking tot deze taken verduidelijk de memorie van toelichting het volgende: *"Gegevensattestering wordt toegevoegd als eerste taak genoemd in artikel 4. In het licht van de lopende en toekomstige projecten in toepassing van de voorgestelde wijzigingen aan de eIDAS-verordening, zoals de ontwikkeling van de portemonnee voor digitale identiteit, wordt ook overwogen dat burgers attesten zullen kunnen ontvangen die de authenticiteit van overheidsinformatie bevestigen. In de toekomst zal de federale dienstenintegrator dus ook in staat moeten zijn om dit soort informatie ter beschikking te stellen*" (onderstreping toegevoegd door de Autoriteit).

47. De Autoriteit heeft de aanvrager gevraagd naar de reikwijdte van de taak zoals vermeld in overweging 45 (artikel 4, lid 4, van de wet van 2012 zoals gewijzigd door het Wetsontwerp), in het bijzonder met betrekking tot de taak zoals vermeld in artikel 4, lid 5, van de wet van 2012 met betrekking tot de technische modaliteiten en voorwaarden voor communicatie tussen databanken of authentieke bronnen en het netwerk. Richt **artikel 4, lid 4** van de wet zich wel op de toegang tot databanken en authentieke gegevensbronnen? De aanvrager antwoordt als volgt: "*Inderdaad, zoals vermeld in dit artikel, gaat het om de 'toegangskanalen' (tot databanken)*". Artikel 4, lid 4 verduidelijkt echter niet dat het gaat om toegangskanalen "tot databanken".

48. De Autoriteit is van mening dat artikel 4, leden 4 en 5, van de wet van 2012, zoals gewijzigd bij het Wetsontwerp, **zodanig moet worden verduidelijkt dat er een duidelijk onderscheid wordt gemaakt tussen de taken met betrekking tot de uitwisseling van gegevens uit databanken (al dan niet authentieke bronnen) tussen gebruikers en de andere taken met betrekking tot de tenuitvoerlegging van de toekomstige wijziging van de eIDAS-verordening** (waarover de Autoriteit geen uitspraak doet).

49. Ten slotte merkt de Autoriteit met betrekking tot **gegevensintegratie** op dat de aanvrager in artikel 4, lid 8, van de wet van 2012, zoals gewijzigd bij het Wetsontwerp, de mogelijkheid handhaaft om toepassingen te ontwikkelen met het oog op gegevensintegratie. Op dit punt wijst de Autoriteit de aanvrager op de ernstige bedenkingen die zij heeft geuit, met betrekking tot het begrip van databanken uit **authentieke bronnen** dat, *in concreto*, neerkomt op het integreren van gegevens uit authentieke

[28] Artikel 4, lid 4, van de wet van 2012 zoals gewijzigd bij het Wetsontwerp.

bronnen.[29] Met het oog op gegevensbescherming verdient dienstenintegratie de voorkeur boven gegevensintegratie. Hoewel het duidelijk is dat het voorgestelde dispositief op zichzelf juridisch niet kan volstaan als grondslag voor de gegevensverwerking waarop zij betrekking heeft (gegevensintegratie, gegevensaggregatie, gegevensverrijking, enz.), wijst de Autoriteit er niettemin op dat, overeenkomstig de beginselen van voorzienbaarheid en rechtmatigheid[30] , een dergelijke verwerking van persoonsgegevens alleen mag worden uitgevoerd indien het wettelijk kader dat de activiteiten van de gebruiker regelt dit toestaat, en voor zover dit door de wet wordt toegestaan.

**II.3.2. Beschikbaarstelling van herbruikbare toepassingen**

50. In artikel 4, lid 8, van de wet van 2012, zoals gewijzigd door het Wetsontwerp, wordt bepaald dat de dienstenintegrator "*herbruikbare toepassingen ontwikkelt die nuttig zijn voor de integratie, aggregatie, transformatie, verrijking, filtering, anonimisering, pseudonimisering, generalisering, verwijdering, randomisering, beveiligde opslag, verstrekking en uitwisseling van in databanken opgeslagen gegevens*" (onderstreping toegevoegd door de Autoriteit).

51. Bovenal is de Autoriteit, net als de Raad van State[31], van mening dat het dispositief van het Wetsontwerp zelf de **beoogde gegevensverwerking moet definiëren**, in het licht van de toelichting (integratie, aggregatie, transformatie, enz.).

52. De memorie van toelichting verduidelijkt vervolgens als volgt:

> *"De bewaring betreft de tijdelijke bewaring en is daarom een algemene voorziening voor tijdelijke caching. Het gaat dus geenszins om permanente bewaring van gegevens. Het betreft uitsluitend tijdelijke technische opslag om bijvoorbeeld attesten te kunnen afgeven of identificatiecertificaten te kunnen opstellen. Gegevens worden alleen opgeslagen als ze nodig zijn voor verwerking, en de tijdelijke opslagperiode is beperkt tot maximaal 5 dagen en wordt bepaald op basis van de door de gebruiker gevraagde verwerking. Het verstrekken en uitwisselen van gegevens spreekt voor zich.*
>
> *Gebruikers kunnen, eventueel op verzoek van een bevoegde instantie, ervoor kiezen om de bovenvermelde toepassingen van de federale dienstenintegrator te gebruiken*" (onderstreping toegevoegd door de Autoriteit).

[29] Zie recentelijk de overwegingen 65-71 van advies 154/2023.

[30] Zie voetnoten nrs. 13-14.

[31] P. 5 van voornoemd advies.

53. In deze context heeft de Autoriteit de aanvrager ondervraagd over de vraag of het uitsluitend gaat om de ontwikkeling van software (programma's) of dat er ook sprake is van dienstverlening. Zij heeft de aanvrager ook gevraagd naar de betekenis van het "*herbruikbare*" karakter van de betrokken toepassingen.

54. De aanvrager antwoordde als volgt:

> *"Artikel 4, lid 8 betreft expliciet de opdracht voor ontwikkeling. De (eventuele) terbeschikkingstelling van deze toepassingen aan gebruikers wordt vermeld in artikel 12, lid 12.*
>
> *Met de term 'Herbruikbaar' willen we duidelijk maken dat het niet de bedoeling is om voor elke gebruiker dezelfde toepassing vanaf nul te ontwikkelen*".

55. Hierdoor kan niet worden vastgesteld of er ook sprake is van het aanbieden van diensten, aangezien de term "ter beschikking stellen" in dit opzicht vaag is. Het is **aan de aanvrager om <u>het dispositief van</u> het Wetsontwerp op dit punt te <u>verduidelijken,</u>** aangezien dit gevolgen heeft voor de verwerking van persoonsgegevens. Terwijl het aanbieden van een toepassing in de vorm van een dienst de verwerking van persoonsgegevens met zich meebrengt, zal dit in principe niet het geval zijn wanneer de aanvrager een applicatie (een computerprogramma) geleverd krijgt die hij zelf op zijn eigen informatiesysteem moet installeren, configureren en bedienen.

56. Bij een tweede ondervraging over deze bepaling en haar relatie tot artikel 4, lid 1, van de wet van 2012 zoals gewijzigd door het Wetsontwerp, heeft de aanvrager met name het volgende geantwoord:

> *"Voor alle duidelijkheid zal als volgt de terbeschikkingstelling van de ontwikkelde toepassingen uitdrukkelijk worden toegevoegd in 4, lid 4 en 4, lid 8, en wordt de tekst van 4, lid 12 als volgt aangepast:*
>
> *"lid 4 het uitwerken van de technische modaliteiten om de toegangskanalen zo efficiënt en veilig mogelijk uit te bouwen; het uitwerken van de technische modaliteiten en de voorwaarden om de toegangskanalen, waaronder webdiensten, mobiele applicaties, de Europese portemonnee voor digitale identiteit en online portalen, zo efficiënt en veilig mogelijk uit te bouwen, met elkaar te verbinden <u>en ter beschikking te stellen</u>;"*
>
> *"lid 8 het ontwikkelen <u>en het ter beschikking stellen</u> van herbruikbare toepassingen die nuttig zijn voor de integratie, de aggregatie, de transformatie, de verrijking, de filtering, de anonimisering, de pseudonimisering, de veralgemening, de schrapping, de randomisering, de*

*beveiligde bewaring, terbeschikkingstellingstelling en uitwisseling van in de gegevensbanken opgeslagen gegevens;"*

*"lid 12 het ontwikkelen, het testen, het onderhouden, het corrigeren en het ter beschikking stellen van de toepassingen en de systemen die nodig zijn om de voorgaande opdrachten te realiseren en de verwerking van de gegevens uit de gegevensbanken die daarvoor nodig zijn*;"
".

57. De Autoriteit neemt kennis van deze wijzigingen. De Autoriteit wijst echter de aanvrager op het feit dat deze wijzigingen niet volledig tegemoetkomen aan alle opmerkingen van de Autoriteit. Bovendien merkt zij op dat in lid 4 de passage "*het uitwerken van de technische modaliteiten om de toegangskanalen zo efficiënt en veilig mogelijk uit te bouwen*" redundant lijkt.

### II.3.3. Elektronische identificatie en de eIDAS-verordening

58. Het is ook de dienstenintegrator die "*elektronische verbindingsdiensten ter beschikking stelt voor publieke toepassingen binnen de authenticatiedienst, overeenkomstig artikel 9* [32] *van de wet van 18 juli 2017 betreffende de elektronische identificatie en de toepassingen en systemen die nodig zijn voor de werking van deze authenticatiedienst en de identificatiesystemen zoals voorzien in Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG*" (onderstreping toegevoegd door de Autoriteit). De memorie van toelichting verduidelijkt dat de toevoeging door het Wetsontwerp "*de dienstenintegrator in staat stelt om klaar te zijn voor onder andere interacties met de Europese portemonnee voor digitale identiteit, voor identiteitsmatching, voor attribuutvalidatie, ...*". (onderstreping toegevoegd door de Autoriteit). In dit verband heeft de Autoriteit de aanvrager ondervraagd of de toevoeging verder reikt dan de tenuitvoerlegging van de eIDAS-verordening en de hervorming ervan, en zo ja, op welke manier. De aanvrager antwoordde als volgt: "*Correct, ze beperkten zich tot het anticiperen op de tenuitvoerlegging van de hervorming van de eIDAS-verordening*".

59. **De Autoriteit,** die haar analyse op dit punt voorbehoudt om de eerder genoemde reden, is daarom van mening dat **expliciet moet worden verwezen naar de desbetreffende diensten van de hervormde eIDAS-verordening en de bepalingen die daarin voorzien**.

---

[32] Deze bepaling luidt als volgt:

*"1. Onverminderd de verplichtingen verbonden aan Verordening (EU) 910/2014 is de Federale Overheidsdienst Strategie en Ondersteuning verantwoordelijk voor het aanbieden van elektronische identificatiediensten voor publieke toepassingen binnen de authenticatiedienst*

*§ 2 De Federale Overheidsdienst Strategie en Ondersteuning verzekert de beschikbaarheid van de authenticatiedienst.*

*§ 3 De Federale Overheidsdienst Strategie en Ondersteuning heeft het recht om het identificatienummer van natuurlijke personen ingeschreven in het Rijksregister te gebruiken om zijn authenticatietaken uit te voeren.*

**II.3.4. <u>Verordening nr. 2018/1724</u>**

60. De dienstenintegrator "*levert applicaties en systemen voor gegevensuitwisseling om de doelstellingen te bereiken die zijn vastgelegd in*" Verordening 2018/1724.

61. De Autoriteit is opnieuw van mening dat **<u>deze bepaling moet verwijzen naar de relevante bepalingen van Verordening 2018/1724 om</u>** precies te kunnen vaststellen wat eronder valt.

**II.3.5. <u>Ontwikkeling, testen en onderhoud van toepassingen en systemen</u>**

62. Artikel 4, lid 12, van de wet van 2012 zoals gewijzigd door het Wetsontwerp voorziet dat de dienstenintegrator "*de toepassingen en systemen die nodig zijn om de voormelde taken uit te voeren, ontwikkelt, test, onderhoudt, corrigeert en ter beschikking stelt en de gegevens verwerkt in de databanken die daarvoor nodig zijn*". In de memorie van toelichting bij dit artikel wordt het volgende verduidelijkt: "*Verder wordt gespecificeerd dat de dienstenintegrator, om <u>alle taken te</u> vervullen, applicaties en systemen moet <u>ontwikkelen, testen, corrigeren en beschikbaar stellen</u> en daarvoor de relevante gegevens moet gebruiken. Voor zover mogelijk zijn dit <u>testgegevens, indien beschikbaar bij de gebruiker</u>, en geen echte gegevens. Als op verzoek van de gebruiker tests moeten worden uitgevoerd <u>met echte gegevens</u>, moeten de nodige maatregelen worden genomen om deze te beschermen in overeenstemming met* [de] *AVG*" (onderstreping toegevoegd door de Autoriteit).

63. De Autoriteit heeft de aanvrager ondervraagd over de reikwijdte en de toegevoegde waarde van een dergelijke bepaling, die in zekere zin overlappend lijkt te zijn met de verwijzende bepalingen. Vereist het bijvoorbeeld dat de dienstenintegrator de betrokken toepassingen zelf ontwikkelt (zonder uitbesteding)? Is het doel om het verwerken van persoonsgegevens voor testdoeleinden[33] te reguleren? De aanvrager antwoordde dat het niet de bedoeling is om het gebruik van onderaanneming te verbieden, evenals het volgende:

> ***"De uitvoering van de taken*** *van de federale dienstenintegrator* ***vereist een aantal verwerkingshandelingen waarvoor het passend was om ze expliciet te vermelden om discussies over de doeleinden van*** *de verwerkingshandelingen, zoals de ontwikkeling, het testen, het onderhoud, de correctie en de terbeschikkingstelling van toepassingen en systemen, te* ***vermijden.***
> *De vermelding van tests op zich is uiteraard onvoldoende om de mogelijke verwerking van persoonsgegevens in het kader van tests te rechtvaardigen, maar geeft duidelijk aan dat tests*

[33] Over de verdere verwerking van persoonsgegevens voor testdoeleinden, zij het in een andere context dan die van de overheidssector, zie HvJEU (1e Kamer), arrest van 20 oktober 2022, *Digi/Nemzeti Adatvédelmi és Információszabadság Hatóság*, zaak C-77/21.

*integraal deel uitmaken van de taken van de FOD BOSA. Voor elke mogelijke (en uitzonderlijke) verwerking van persoonsgegevens in het kader van tests moeten alle beginselen van de AVG worden toegepast, waaronder uiteraard het beginsel van gegevensminimalisatie*" (vetgedrukt door de Autoriteit).

64. **De Autoriteit ziet echter niet de juridische meerwaarde van artikel 4, lid 12, van de wet van 2012, waarvan de reikwijdte onduidelijk blijft**. Om een van zijn taken uit te voeren, moet een dienstenintegrator ofwel een systeem of applicatie opzetten en implementeren. Dit impliceert dan dat hij het moet ontwikkelen, testen en onderhouden. Ofwel het doel van de bepaling is om een specifieke verwerking van persoonsgegevens toe te staan, in welk geval de bepaling veel te vaag is omdat zij niet de essentiële elementen bepaalt van de verwerking die zij beoogt toe te staan (in overeenstemming met de beginselen van voorzienbaarheid en rechtmatigheid waarnaar elders wordt verwezen). In haar huidige formulering kan een dergelijke bepaling geen enkel nuttig effect hebben met betrekking tot de vraag of tests al dan niet kunnen worden uitgevoerd met behulp van "echte" gegevens[34] (een kwestie die in de memorie van toelichting aan de orde wordt gesteld). Het spreekt voor zich dat het nog minder de verwerking van persoonsgegevens kan toestaan in het kader van de ontwikkeling van intelligente systemen of systemen op basis van *datamining*. De vraag hoe tests en ontwikkelingen kunnen worden uitgevoerd, hangt af van het normatieve kader dat van toepassing is op de taken van algemeen belang waarvoor het systeem in kwestie wordt ontwikkeld. Gegeven dit normatieve kader, als het noodzakelijk is om persoonsgegevens te verwerken om tests uit te voeren, zal deze verwerking worden toegestaan door de AVG. In deze omstandigheden is **de Autoriteit van mening dat de voorgestelde bepaling ofwel moet worden geschrapt ofwel moet worden ontwikkeld, waarbij zij zich haar analyse voorbehoudt voor het laatste**.

### II.3.6. Verordening datagovernance

65. De dienstenintegrator "*vervult de rol van centraal informatiepunt en bevoegde instantie voor technische bijstand als bedoeld in respectievelijk artikel 8 en artikel 7, lid 1*"[35] van de verordening datagovernance. Deze taak geeft geen aanleiding tot bijzondere opmerkingen van de Autoriteit.

---

[34] Deze kwestie moet worden opgelost door de voor de verwerking verantwoordelijke, met name in het licht van het beginsel van gegevensminimalisering en het regelgevingskader dat *in concreto* van toepassing is op de betrokken taak en verwerking. De bepaling in het Wetsontwerp is te vaag en algemeen om in dit opzicht enig rechtsgevolg te hebben.

[35] De federale dienstenintegrator zal dus een rol spelen in het beschikbaar stellen van gegevens die, hoewel ze niet beschikbaar kunnen worden gesteld op grond van de Hergebruikrichtlijn en de omzetting ervan in Belgisch recht, toch beschikbaar kunnen worden gesteld op grond van de Belgische wettelijke regels ter uitvoering van de Data Governance Verordening. Over het hergebruik van overheidsdocumenten en deze verordening, zie advies nr. 143/2023 van de Autoriteit, hierboven geciteerd, overweging 73 e.v. In dit verband bestaat de betrokken bijstand overeenkomstig artikel 7, lid 4, van dezelfde verordening met name uit :

*"a) technische bijstand te verlenen door een beveiligde verwerkingsomgeving beschikbaar te stellen om toegang te geven tot het hergebruik van gegevens;*

*b) begeleiding en technische bijstand bieden over hoe gegevens het beste kunnen worden gestructureerd en opgeslagen om ze gemakkelijk toegankelijk te maken;*

### II.3.7. Gegevensuitwisseling met andere dienstenintegratoren

66. Tot slot bepaalt artikel 4, lid 14, van de wet van 2012 zoals gewijzigd door het Wetsontwerp dat de dienstenintegrator gegevens moet uitwisselen met andere dienstenintegratoren. In de memorie van toelichting staat hierover het volgende: *"De dienstenintegrator wisselt gegevens uit met de andere dienstenintegratoren, die op hun beurt de integratie van diensten en de geïntegreerde levering van gegevens organiseren. Er wordt ook samengewerkt in het kader van de 'G-Cloud', een samenwerkingsverband dat de samenwerking op het vlak van ICT-infrastructuur tussen federale overheidsdiensten wil maximaliseren.*" De Autoriteit heeft de aanvrager gevraagd wat de "G-Cloud" inhoudt en welk normatieve kader daarop van toepassing is. De aanvrager heeft aanvankelijk als volgt geantwoord:

> *"G-Cloud is een gezamenlijk initiatief van de Federale Overheidsdiensten (FOD), de Openbare Instellingen voor Sociale Zekerheid (OISZ) en de IT-organisaties binnen de Belgische overheid. Het staat ten dienste van en onder toezicht van de deelnemende instellingen. De samenwerking tussen deze instellingen is gebaseerd op hun respectieve expertisedomeinen. Meer informatie is hier te vinden: https:*//www.gcloud.belgium.be/nl/home. Vervolgens legde hij uit:
>
> *"We hebben geen informatie over een wettelijk kader voor de G-cloud. De G-cloud wordt enkel informatief vermeld in de memorie van toelichting van dit Wetsontwerp. We stellen voor om de vermelding van de G-Cloud in de memorie van toelichting te schrappen*" (vetgedrukt door de Autoriteit).

67. De Autoriteit **neemt kennis van het voornemen van de aanvrager om de verwijzing naar de G-Cloud uit de memorie van toelichting te schrappen**. De Autoriteit is tevens van mening dat **de verwijzing naar de G-Cloud** (waarvoor zij het normatieve kader niet heeft onderzocht) **inderdaad moet worden weggelaten**. De G-Cloud, waarnaar in het Wetsontwerp niet expliciet wordt verwezen (de bepaling waarover opmerkingen zijn gemaakt, verwijst naar dienstenintegratoren,

---

*c) technische ondersteuning te bieden voor pseudonimisering en ervoor te zorgen dat gegevens zodanig worden verwerkt dat de persoonlijke levenssfeer, de vertrouwelijkheid, de integriteit en de toegankelijkheid van de informatie in de gegevens waarvoor hergebruik is toegestaan, effectief worden beschermd, met inbegrip van technieken voor anonimisering, veralgemening, verwijdering en randomisering van persoonsgegevens of andere moderne methoden ter bescherming van de persoonlijke levenssfeer, en de verwijdering van commercieel vertrouwelijke informatie, met inbegrip van bedrijfsgeheimen of inhoud die wordt beschermd door intellectuele-eigendomsrechten;*

*d) openbare lichamen, waar passend, bijstand te verlenen aan hergebruikers bij het verkrijgen van toestemming voor hergebruik van betrokkenen of van toestemming van de houders van gegevens overeenkomstig hun specifieke besluiten, ook met betrekking tot het grondgebied waar de gegevensverwerking zal plaatsvinden, en openbare lichamen bij te staan bij het opzetten van technische mechanismen voor de doorzending van verzoeken om toestemming of toestemming van hergebruikers, waar dit praktisch haalbaar is;*

*e) bijstand te verlenen aan openbare lichamen bij de beoordeling van de toereikendheid van de contractuele verbintenissen die een hergebruiker krachtens artikel 5, lid 10, is aangegaan.*

een categorie waartoe de G-Cloud niet a *priori* lijkt te behoren), lijkt een onderwerp op zich te zijn dat een aanvullende specifieke analyse vereist vanuit het oogpunt van gegevensbescherming.

### II.3.8. Artikel 4, lid 1, van de wet van 2012 en de algemene rol van de dienstenintegrator

68. Meer in het algemeen is de Autoriteit, in het licht van het voorgaande, van mening dat lid 1 van artikel 4 van de wet van 2012 moet worden **geherformuleerd om rekening te houden met de nieuwe taken die worden toegewezen aan de federale dienstenintegrator, op basis van duidelijke concepten of, in ieder geval, concepten die in het Wetsontwerp zijn gedefinieerd**. Op dit punt zou dit lid bijvoorbeeld kunnen worden gelezen als een verwijzing naar een derde type van integratie, de integratie van "*gegevensverwerkingsprocessen*", naast gegevensintegratie en dienstenintegratie, hoewel de concrete reikwijdte van dit concept niet wordt gedefinieerd in het Wetsontwerp. Opmerking: in deze context moet ook rekening worden gehouden met de volgende opmerkingen over de "gebruikersovereenkomst".

### II.4. Facultatief karakter van het gebruik van de diensten van de federale dienstenintegrator

69. Zoals gewijzigd door het Wetsontwerp, handhaaft artikel 4 van de wet van 2012 het beginsel dat **het gebruik van de federale dienstenintegrator niet bindend is**: "*De federale dienstenintegrator heeft tot taak, met de instemming van de gebruikers en andere dienstenintegratoren, de gegevensverwerkingsprocessen te integreren en binnen dit kader gegevens op geïntegreerde wijze toegankelijk te maken*" (onderstreping toegevoegd door de Autoriteit). Zoals voorzien in het dispositief van de wet van 2012 geldt het vereiste van de noodzaak van deze overeenkomst voor alle taken van de federale dienstenintegrator. Bovendien vereist de tussenkomst van laatstgenoemde de sluiting van een overeenkomst (een conventie) overeenkomstig artikel 5, § 2, van de wet van 2012, zoals gewijzigd door het Wetsontwerp. Concreet betekent dit bijvoorbeeld dat de betrokken overheidsdiensten niet wettelijk verplicht moeten zijn om gebruik te maken van de diensten van de integrator door de wet van 2012, net zoals de rechthebbenden.

70. **De Autoriteit heeft de aanvrager hierover ondervraagd, met name wat betreft de wettelijke regeling die van toepassing is op deze overeenkomst en de reikwijdte ervan** (*wat gebeurt er* als een overheidsdienst niet langer gebruik wenst te maken van alle of een deel van de diensten van de federale dienstenintegrator? Wat is de reikwijdte van de gegeven overeenkomst)? Ze heeft ook vragen gesteld over **de interactie tussen dit principe en de nieuwe taken van de integrator** (bijvoorbeeld voor artikel 4, lid 10, zoals gewijzigd door het Wetsontwerp, betreffende elektronische identificatie, zullen de diensten van de integrator *a priori* onvermijdelijk zijn). De

noodzaak van een voorafgaand akkoord is dus een voorwaarde voor de toepassing van artikel 8 van het Wetsontwerp.

71. De aanvrager antwoordde als volgt:

> *"Zoals voorzien door de wet, is de instemming van de gebruiker opgenomen in een gebruikersovereenkomst of gebruiksvoorwaarden, afhankelijk van de gebruikerscategorie.*
>
> ***Een gebruikersovereenkomst** tussen FOD BOSA en een specifieke gebruiker beschrijft de concrete samenwerking tussen de partijen, **met expliciete vermelding van de betreffende diensten die worden geleverd**. Zo om**vat de gebruikersovereenkomst zowel de rechten als de verplichtingen van de betrokken partijen krachtens de wet van 2012**, alsook **de aanvullende afspraken die nodig zijn om de rechten, verplichtingen en verantwoordelijkheden te definiëren**. Concreet betreft dit met name de beschrijving van service level agreement, bepalingen met betrekking tot audit trails (overeenkomstig artikel 14 van de wet van 2012). Met betrekking tot de gegevensuitwisseling bevat de gebruiksovereenkomst met de verantwoordelijke voor de authentieke bron ook de specifieke voorwaarden voor de verwerking van persoonsgegevens in het kader van de tussenkomst van de federale dienstenintegrator. Dit omvat in het bijzonder: de identificatie van de gegevensbron, de rechtsgrondslag voor de bevoegdheid van de gegevensbron of het wettelijk kader van de betrokken gegevensbron, de categorieën van persoonsgegevens, de categorieën van betrokken personen, de rechtsgrondslag voor de communicatie (tussen bron en ontvanger) of de categorieën van toestemming die vereist zijn voor deze communicatie (bv. protocol, besluit, specifieke toestemming, enz.), de aard van de verwerking door de dienstenintegrator, de toegangskanalen voor het ter beschikking stellen van de gegevens, enz.*
>
> ***De geleverde diensten en de gebruiksvoorwaarden van deze diensten worden daarom uitdrukkelijk gespecificeerd in de gebruikersovereenkomst. Indien de** samenwerking in kwestie wordt beëindigd, wordt de gebruikersovereenkomst beëindigd*" (onderstreping toegevoegd door de Autoriteit).

72. **De Autoriteit is van mening dat het Wetsontwerp moet worden <u>verduidelijkt met betrekking tot de mogelijke grenzen van het niet-bindende karakter van het gebruik van het geheel of een gedeelte van de diensten van de federale dienstenintegrator</u>**. Uit het Wetsontwerp moet duidelijk blijken dat de verplichtingen die in de wet van 2012 zijn vastgelegd met betrekking tot de taken van de dienstenintegrator, **alleen van toepassing zijn wanneer de gebruiker er vrij voor kiest om gebruik te maken van de relevante diensten van de federale dienstenintegrator**.

73. Heel concreet, bijvoorbeeld met betrekking tot **de uitwisseling van gegevens tussen gebruikers** (en in het bijzonder overheidsinstanties; de **oorspronkelijke taak van de dienstenintegrator**), betekent dit in het kader van **artikel 8 van de wet van 2012 dat** als een gebruiker een dienst van de dienstenintegrator gebruikt om toegang te krijgen tot een authentieke gegevensbron, dit niet betekent dat de gebruiker verplicht is om de andere diensten van de dienstenintegrator te gebruiken om toegang te krijgen tot andere gegevens die via deze diensten beschikbaar zijn en die voor deze gebruiker noodzakelijk zouden zijn om zijn taken uit te voeren. In de overeenkomst tussen de gebruiker en de dienstenintegrator zal worden bepaald tot welke gegevens de gebruiker toegang zal hebben via de diensten van de integrator. Deze aanpak is vooral belangrijk omdat gegevens uit niet-authentieke bronnen ook via de dienstenintegrator kunnen worden geraadpleegd.

74. Er moet ook worden opgemerkt dat **het niet kan worden uitgesloten dat het normatieve kader dat van toepassing is op een overheidsinstantie, haar verplicht om gebruik te maken van bepaalde diensten die beschikbaar zijn via de federale dienstenintegrator**[36] .

75. **Deze benadering van de vrijheid van de gebruiker** om gebruik te maken van de diensten van de integrator krachtens de wet van 2012, onverminderd de bepalingen van de wet die anders van toepassing zijn, **lijkt in overeenstemming met de taken bedoeld in lid 1** (**behalve voor** "gegevensattesten"), lid **4** (**behalve voor** "portemonnees voor digitale identiteit") **en lid 8, van artikel 4 van de wet van 2012, zoals gewijzigd door het Wetsontwerp**.

76. Dit gezegd zijnde, **vraagt** de Autoriteit **zich af of het behoud van het niet-bindende karakter van het gebruik van de diensten van de integrator relevant en houdbaar blijft met betrekking tot een deel van de nieuwe taken van de dienstenintegrator**. Deze vraag rijst specifiek met betrekking tot elektronische identificatie en de uitvoering van de bepalingen van het Europese recht (nl. lid **1** (**enkel voor** "gegevensattesten"), lid **4** (**enkel voor** "portemonnees voor digitale identiteit"), lid **10, lid 11 en lid 13, van** artikel 4 van de wet van 2012 zoals gewijzigd door het Wetsontwerp).

77. Wat betreft de elektronische identificatie, lijkt het, gezien het feit dat de relevante dienst wordt aangeboden door de dienstenintegrator en geen andere entiteit, dat gebruikers niet vrij zijn om te kiezen of ze al dan niet gebruikmaken van de diensten van de integrator voor elektronische identificatie. Met betrekking tot de gegevensattestering, hoewel de Autoriteit zich haar analyse voorbehoudt over de tenuitvoerlegging van de hervorming van de eIDAS-verordening, rijst dezelfde

[36] Zie bijvoorbeeld overweging 47 van advies nr. 82/2023 van 27 april 2023 *betreffende een voorontwerp van wet over de oprichting en het beheer van de federale leerrekening (CO-A-2023-052)*.

vraag: wordt op Europees niveau overwogen om een onmisbare rol toe te kennen aan de federale dienstenintegrator of zal elke betrokken overheidsinstantie in deze kwestie vrij blijven?

78. Met andere woorden, en nogmaals, **het dispositief van het Wetsontwerp moet duidelijk maken wat de reikwijdte is van de "*overeenkomst*" die de gebruiker moet sluiten**. In plaats van vrij te zijn om al dan niet gebruik te maken van de diensten van de integrator, kan de gebruiker **verplicht worden om een overeenkomst aan te gaan met de dienstenintegrator**.

79. Concluderend is de Autoriteit van mening dat **het dispositief van artikel 8 van de wet van 2012, zoals gewijzigd door het Wetsontwerp** (en, in voorkomend geval, de memorie van toelichting), moet **worden aangepast om duidelijk de omvang van de vrijheid van de gebruikers te bepalen** met betrekking tot de verschillende taken van de federale dienstenintegrator.

## II.5. Verantwoordelijkheden met betrekking tot de verwerking

### II.5.1. Verantwoordelijkheden van de dienstenintegrator en van de gebruikers

80. Artikel 15 van het Wetsontwerp legt de **verantwoordelijkheden voor gegevensverwerking vast**. De Autoriteit herinnert aan haar vaste adviespraktijk waarin wordt gesteld dat een overheidsinstantie (of een private entiteit) in beginsel **verantwoordelijk is voor de verwerking van gegevens die noodzakelijk is voor de uitvoering van haar openbare taken (of die onder de bevoegdheid vallen van de betreffende overheidsinstantie)[37], of die noodzakelijk is voor de nakoming van de wettelijke verplichting waaraan zij krachtens de** betrokken norm **is gebonden [38] [39],**

[37] Artikel 6, lid 1, onder e), van de AVG.

[38] Artikel 6, lid 1, onder c), van de AVG.

[39] Zie in het bijzonder: Advies nr. 143/2023 van 29 september 2023 *betreffende een voorontwerp van decreet houdende instemming met het samenwerkingsakkoord tussen het Waals Gewest en de Franse Gemeenschap tot aanwijzing van de dienstintegrator van het Waals Gewest en de Franse Gemeenschap en een ontwerp van samenwerkingsakkoord met betrekking tot de oprichting van de gemeenschappelijke dienst van de Advies 154/2023 - 6/80 Waalse Regeringen en de Franse Gemeenschap, genaamd Banque Carrefour d'échange de données (niet onderworpen aan instemming) (CO-A-2023-375), en betreffende een ontwerp van decreet houdende instemming met het samenwerkingsakkoord tussen het Waals Gewest en de Franse Gemeenschap tot aanwijzing van de dienstintegrator van het Waals Gewest en de Franse Gemeenschap en een ontwerp van samenwerkingsakkoord met betrekking tot de oprichting van de gemeenschappelijke dienst van de Waalse Regeringen en de Franse Gemeenschap, genaamd Banque Carrefour d'échange de données (niet onderworpen aan instemming) (CO-A-2023-376) (hierna «advies 143/2023»)* overweging 7 e.v. Advies nr. 83/2023 van de Autoriteit van 27 april 2023 *betreffende een voorontwerp van ordonnantie tot wijziging van de ordonnantie van 4 april 2019 betreffende het platform voor de elektronische uitwisseling van gezondheidsgegevens (CO-A-2023-147)*, overweging nr. 11; Advies nr. 129/2022 van 1er juli 2022 *betreffende de artikelen 2 en 7 tot 47 van een wetsontwerp houdende diverse bepalingen in verband met de economie*, overwegingen nr. 42 e.v. Advies nr. 227/2022 van 29 september 2022 *betreffende een voorontwerp van decreet over open data en het hergebruik van overheidsinformatie (CO-A-2022-209)*, overwegingen 17-23; Advies nr. 131/2022 van 1er juli 2022 *betreffende een wetsontwerp tot oprichting van de Commission du travail des arts en tot verbetering van de sociale bescherming van werknemers in de kunsten*, overwegingen 55 e.v. Advies nr. 112/2022 van 3 juni 2022 *inzake een wetsontwerp tot wijziging van het Sociaal Strafwetboek met het oog op de oprichting van het eDossierplatform*, overwegingen 3-41 en 87-88; Advies nr. 231/2021 van 3 december 2021 *inzake een voorontwerp van ordonnantie betreffende de interoperabiliteit van elektronische tolheffingssystemen voor het wegverkeer*, overwegingen 35-37; Advies nr. 37/2022 van 16 februari 2022 *over een voorontwerp van decreet tot oprichting van het gecentraliseerde platform voor geautomatiseerde gegevensuitwisseling "E-Paysage"*, overweging 22; Advies nr. 13/2022 van 21 januari 2022 *betreffende een ontwerp van besluit van de Brusselse Hoofdstedelijke Regering houdende de toekenning van premies voor de verbetering van de huisvesting en een ontwerp van besluit van de*

**40**. Ze benadrukt ook de conformiteit van deze praktijk met het recente arrest van het Hof van Justitie (3e kamer) van 11 januari 2024, *Belgische Staat tegen de Gegevensbeschermingsautoriteit* , zaak C-231/22, betreffende de aansprakelijkheid van het Belgisch Staatblad.

81. **Artikel 15, lid 1,** van de wet van 2012, zoals gewijzigd bij het Wetsontwerp, **is rechtstreeks in overeenstemming met deze logica**, wat de aansprakelijkheid van de dienstenintegrator betreft, en behoeft daarom geen commentaar van de Autoriteit.

82. **Artikel 15, lid 2,** van de wet van 2012, zoals gewijzigd bij het Wetsontwerp, bepaalt daarentegen als volgt: "*Tenzij anders bepaald, is de in artikel 2, lid 10, onder a) tot en met g), bedoelde gebruiker, die verantwoordelijk is voor het beheer van authentieke bronnen of gegevensbronnen, de voor de verwerking verantwoordelijke voor verwerkingen die bestaan uit het verzamelen, opslaan, beheren en verstrekken van persoonsgegevens in de bronnen*" (onderstreping toegevoegd door de Autoriteit).

83. Opnieuw is de Autoriteit van mening dat deze bepaling **in overeenstemming is met haar advies** met betrekking tot de verantwoordelijkheden ten aanzien van gegevensverwerking. In een context als de onderhavige komt het vaststellen van een verantwoordelijkheid met betrekking tot de verwerking neer op het vaststellen van een essentieel element van de verwerking op een zodanige wijze dat alleen een **norm met de status van wet** dit kan doen. Met andere woorden, de bepaling moet van toepassing zijn **tenzij er in beginsel een andersluidende bepaling in een wet** (wet, decreet of beschikking) is. In feite is het de bedoeling om in beginsel te verwijzen naar een bepaling met de status van wet, aangezien het de bedoeling is dat de diensten van de federale integrator ook beschikbaar zijn voor de deelentiteiten.

84. Ten tweede benadrukt de Autoriteit dat in beginsel **deze verantwoordelijkheid moet zijn vastgelegd in** (of duidelijk moet voortvloeien uit) **het *normatieve kader dat van toepassing is op de* betrokken gegevensbron (al dan niet authentiek)**. Niettemin begrijpt de Autoriteit dat de aanvrager een aanvullende juridische zekerheid bedoelt in het kader van de toepassing van het dispositief van het Wetsontwerp. Bovendien zou het, met name in de context van deelentiteiten, ook niet uitgesloten zijn dat het recht van de deelentiteit ook voorziet in bijkomende verantwoordelijkheid van de eigen dienstenintegrator in interacties met de federale dienstenintegrator (in welk geval bijvoorbeeld de persoon die verantwoordelijk is voor het beheer van de authentieke gegevensbron niet langer alleen verantwoordelijk zou zijn voor het ter beschikking stellen van de gegevens).

---

*Brusselse Hoofdstedelijke Regering tot wijziging van het besluit van de Brusselse Hoofdstedelijke Regering van 9 februari 2012 houdende de toekenning van financiële steun voor energie*, overwegingen 9-17.

[40] Advies nr. 154/2023 van 20 oktober 2023 *betreffende een voorontwerp van gemeenschappelijk decreet en ordonnantie tot vaststelling van de code voor Brusselse governance en gegevens (CO-A-2023-407)*, overweging 167.

85. Ten derde was de Autoriteit, in het kader van een hervorming van de Waalse wetgeving inzake de uitwisseling van gegevens uit authentieke bronnen, van oordeel dat de authentieke gegevensbron en de dienstenintegrator **gezamenlijk verantwoordelijk zijn** voor de verwerking van de van gegevens aan de deelnemende overheidsdiensten[41]. De Autoriteit is van mening dat **deze overwegingen *mutatis mutandis van toepassing zijn in het kader van* het onderhavige Wetsontwerp**, ook met betrekking tot niet-authentieke gegevensbronnen die beschikbaar worden gesteld via de federale dienstenintegrator.

86. **Artikel 9 van de wet van 2012, zoals gewijzigd door het Wetsontwerp, is volledig in lijn met deze logica** door te voorzien in **een controleverplichting voor de federale dienstenintegrator**. Volgens deze bepaling "*onderzoekt de federale dienstenintegrator voor elk verzoek om raadpleging of mededeling of de aanvrager en het verzoek in kwestie voldoen aan de regels van de betrokken databank of authentieke bron of aan de regels die van toepassing zijn op de systemen die door de federale dienstenintegrator worden beheerd in het kader van zijn taken zoals bepaald in artikel 4*" (onderstreping toegevoegd door de Autoriteit). **De Autoriteit merkt terloops op dat artikel 9 van de wet van 2012 moet worden aangevuld om de gevolgen van dit onderzoek te specificeren** (zo zal een niet-conforme aanvraag *a priori* worden afgewezen) **en de mogelijke rol van de gegevensbron waartoe** een gebruiker toegang wil krijgen.

87. **In dezelfde context voorziet artikel 8, § 2, van de wet van 2012, zoals gewijzigd door het Wetsontwerp**, dat: "*Indien de mededeling van persoonsgegevens tussen gebruikers onder de toepasselijke wettelijke voorwaarden een overeenkomst of machtiging van een bevoegde instantie vereist, de federale dienstenintegrator de gevraagde persoonsgegevens mededeelt voor zover er een overeenkomst of machtiging bestaat, zelfs indien de uitwisseling via de federale dienstenintegrator daarin niet uitdrukkelijk is voorzien*" (onderstreping toegevoegd door de Autoriteit). De Autoriteit is ook van mening dat het Wetsontwerp op dit punt moet verduidelijken **dat het inderdaad aan de dienstenintegrator is om voor elk verzoek om gegevensverstrekking na te gaan of een dergelijke overeenkomst of machtiging al dan niet vereist is**.

88. **Artikel 14 van de wet van 2012, zoals gewijzigd bij het Wetsontwerp**, betreffende gegevensbeveiliging **sluit verder aan bij deze logica van gezamenlijke verantwoordelijkheid** door te voorzien in een gezamenlijke verplichting voor de gebruiker en de dienstenintegrator[42] .

89. **In de memorie van toelichting staat** echter **duidelijk dat er "drie afzonderlijke verantwoordelijken voor de verwerking" zijn**. De Autoriteit is van mening dat **het Wetontwerp op dit punt moet worden aangepast.**

[41] Zie de overwegingen 12-14 van Advies nr. 143/2023.

[42] Zie overwegingen 123 e.v.

90. Het Wetsontwerp wijzigt voorts **artikel 6 van de wet van 2012** door te bepalen dat **de Koning voortaan**, onverminderd de specifieke wetgeving ter zake, bij een in ministerraad overlegd besluit het verzamelen en het bewaren van authentieke gegevens functioneel ***kan*** **(in plaats van** *moet***) her**verdelen. In de memorie van toelichting staat hierover het volgende: "*Artikel 6 voorziet dat de Koning het verzamelen en bewaren van authentieke gegevens functioneel kan herverdelen. Tot nu toe is dit niet gebeurd omdat het niet nodig is gebleken; het moet daarom worden beperkt tot een mogelijkheid*" (onderstreping toegevoegd door de Autoriteit). De Autoriteit vroeg de aanvrager of de reden waarom dit niet nodig was, verband hield met de elders geldende normatieve kaders. De aanvrager antwoordde als volgt: "*Correct, dit geldt alleen als er een noodzaak is en er nog geen regelgeving van kracht is*".

91. De Autoriteit is van mening dat, op basis van de beginselen, artikel 6 van de wet 2012 inderdaad in beginsel nooit van toepassing zou moeten zijn op de uitwisseling van gegevens uit een **authentieke gegevensbron, aangezien overeenkomstig de beginselen van voorzienbaarheid en rechtmatigheid de essentiële elementen van de betrokken gegevensverwerking (met inbegrip van verzameling en opslag) moeten zijn vastgelegd in de wettelijke norm die van toepassing is op de betreffende authentieke gegevensbron**. Met andere woorden, **de Autoriteit is van mening dat artikel 6 van de wet van 2012 kan worden geschrapt.**

### II.5.2 Coördinatiecomité

92. De Autoriteit heeft de aanvrager gevraagd naar de reikwijdte van artikel 27, lid 3, van de ontwerpwet van 2012, dat als volgt luidt: "*Het Coördinatiecomité beraadslaagt over initiatieven om de samenwerking binnen het netwerk te bevorderen en in stand te houden, en over initiatieven die kunnen bijdragen tot de rechtmatige en vertrouwelijke verwerking van netwerkgegevens*" (onderstreping toegevoegd door de Autoriteit). Zijn er plannen om het Coördinatiecomité in staat te stellen bindende besluiten te nemen ten aanzien van de dienstenintegrator (en, indien van toepassing, zijn gebruikers) op het gebied van de verwerking van persoonsgegevens? De aanvrager antwoordde als volgt: *"Nee, de wet voorziet niet in deze bevoegdheid*". **De Autoriteit neemt nota van dit antwoord en verzoekt de aanvrager de bepaling in het Wetsontwerp, die onduidelijk is** over de rol van het Coördinatiecomité, te **verduidelijken**.

93. Het huidige artikel 33 van de wet van 2012 voorziet al dat het Overlegcomité[43] "*zal beraadslagen over initiatieven om de samenwerking tussen dienstenintegratoren te bevorderen en in stand te houden*" (onderstreping toegevoegd door de Autoriteit). Het Wetsontwerp voorziet verder dat "*het*

[43] Die, onder de wet van 2012, bestaat uit een vertegenwoordiger van de federale dienstenintegrator en een vertegenwoordiger van de verschillende andere dienstenintegratoren.

*Overlegcomité voor dienstenintegratoren tot doel heeft de interconnecties tussen dienstenintegratoren op een optimale en efficiënte manier te organiseren zodat organisaties slechts op één dienstenintegrator een beroep hoeven te doen*" (onderstreping toegevoegd door de Autoriteit). De Autoriteit heeft de aanvrager gevraagd of en in welke mate het de bedoeling was dat het Overlegcomité bindende besluiten zou nemen ten aanzien van dienstenintegratoren en/of gebruikers op het gebied van de verwerking van persoonsgegevens. Hij antwoordde als volgt: *"Nee, de wet voorziet niet in deze bevoegdheid*". De Autoriteit neemt nota van dit antwoord en verzoekt de aanvrager nogmaals om **de bepalingen in het Wetsontwerp te verduidelijken**. Voorts is zij van mening dat in **de memorie van toelichting moet worden bevestigd dat het Coördinatiecomité niet tot taak heeft bindende besluiten te nemen ten aanzien van dienstenintegratoren en/of gebruikers op het gebied van de verwerking van persoonsgegevens**.

### II.6. Rechten van betrokkenen

#### II.6.1. Publicatie van registers door de dienstenintegrator

94. Op het vlak van transparantie benadrukt **de Autoriteit onmiddellijk de toegevoegde waarde van het Wetsontwerp met betrekking tot gegevensbescherming**, met betrekking tot de verplichting voor de federale dienstenintegrator[44] om het "***geïntegreerd register van verwerkingsactiviteiten***"[45] en het "***register van authentieke bronnen***"[46] openbaar ter beschikking te stellen . Dit zijn belangrijke transparantie-instrumenten.

95. Dit gezegd zijnde, **is de Autoriteit van mening dat deze publicatiemaatregel moet worden versterkt**. Zoals hierboven vermeld, beperkt de rol van de dienstenintegrator zich niet tot het beschikbaar stellen van gegevens uit authentieke bronnen, maar omvat deze ook de toegang tot **gegevens uit andere bronnen**. Daarom zou de **dienstenintegrator ook** een afzonderlijk **register moeten publiceren**, vergelijkbaar met het register van authentieke gegevensbronnen.

#### II.6.2. Protocollen, gebruikersovereenkomsten, gebruiksvoorwaarden

96. Artikel 5, § 2, van de wet van 2012, zoals gewijzigd door het Wetsontwerp, luidt als volgt:

---

[44] Artikel 4, lid 9, van de wet van 2012 zoals gewijzigd door het Wetsontwerp.

[45] Of volgens artikel 2, lid 12, van de wet van 2012 zoals gewijzigd door het Wetsontwerp :

"*een geïntegreerd exemplaar van de inhoud van de registers bedoeld in artikel 30 van Verordening (EU) 2016/679 van 27 april 2016 van het Europees Parlement en de Raad betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens, en tot intrekking van Richtlijn 95/46/EG, en die worden bijgehouden door de gebruikers bedoeld in artikel 2, lid 10, a tot g, samengesteld en toegankelijk gemaakt voor het publiek door de federale dienstenintegrator*".

[46] Of volgens artikel 2, lid 13, van de wet van 2012 zoals gewijzigd door het Wetsontwerp :

Een "*register met een lijst van authentieke bronnen, een beschrijving van de gegevens die ze bevatten en een verwijzing naar de toepasselijke wetgeving, opgesteld en toegankelijk gemaakt voor het publiek door de federale dienstenintegrator*".

> *"De interventiemodaliteiten van de federale dienstenintegrator worden vastgelegd in een gebruikersovereenkomst tussen de federale dienstenintegrator en de gebruikers bedoeld in artikel 2, lid 10, a) tot g), en in de gebruiksvoorwaarden ten aanzien van de gebruikers bedoeld in artikel 2, lid 10, h).*
> *Door het sluiten van een gebruiksovereenkomst of het opleggen van gebruiksvoorwaarden is de federale dienstenintegrator vrijgesteld van het sluiten van een protocol zoals bedoeld in artikel 20 van de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens*" (onderstreping toegevoegd door de Autoriteit).

97. De memorie van toelichting verduidelijkt dat "*de gebruikersovereenkomst de bepalingen met betrekking tot de bescherming van persoonsgegevens en andere bepalingen, zoals dienstverleningsniveaus, moet bevatten*". De Autoriteit begrijpt dat het Wetsontwerp op deze manier beoogt om de vermenigvuldiging van formaliteiten die overbodig zouden kunnen zijn, te vermijden. Dit gezegd hebbende, en zoals de aanvrager zelf aangeeft in zijn antwoorden aan de Raad van State[47], vereist het protocol enerzijds een advies van de functionaris voor gegevensbescherming en anderzijds, moet het bovenal worden gepubliceerd.

98. In navolging van de memorie van toelichting (gegevensbeschermingsbepalingen opnemen in de overeenkomsten) en met het oog op transparantie, is de Autoriteit van mening dat **het Wetsontwerp de dienstenintegrator niet kan vrijstellen van het sluiten van protocollen, behalve onder de volgende voorwaarde.** Het moet **voorzien dat, wanneer dergelijke informatie relevant is, de gebruiksvoorwaarden en de overeenkomsten de protocolinformatie bedoeld in artikel 20, § 1, lid 2, van de Wet Bescherming Persoonsgegevens moeten bevatten in een aparte sectie dat moet worden gepubliceerd op de website van de dienstenintegrator**, waarbij deze laatste ook alle afgesloten overeenkomsten beschikbaar kan maken, binnen de door de AVG toegestane grenzen (d.w.z., indien van toepassing, mits voorafgaande anonimisering, met uitzondering van de vermelding van de identiteit van de ondertekenaars, enz, een kwestie die per geval en samen met de betrokken gebruiker moet worden beoordeeld). **Dit is des te belangrijker omdat het in deze overeenkomsten is dat de mate waarin een gebruiker van plan is gebruik te maken van de diensten van de federale dienstenintegrator zal worden gedefinieerd.**

99. Verder wijst de Autoriteit erop dat artikel 38, lid 1, van de AVG bepaalt dat "de *verwerkingsverantwoordelijke en de verwerker ervoor zorgen dat de functionaris voor*

[47] Blz. 6-7 van voornoemd advies.

*gegevensbescherming op passende wijze en tijdig wordt betrokken bij alle aangelegenheden betreffende de bescherming van persoonsgegevens*". De Autoriteit is van mening dat, net als bij de protocollen, de functionaris **voor gegevensbescherming betrokken moet worden bij het opstellen van de bovengenoemde overeenkomsten en gebruiksvoorwaarden**. Dit zijn juridische instrumenten die centraal staan in de werking van de federale dienstenintegrator.

**II.6.3. Toegang en rectificatie**

***a) Wetsontwerpbepaling***

100. Zoals gewijzigd door het Wetsontwerp, luidt artikel 16 van de wet van 2012 als volgt:

> *"§ 1. Tenzij in bijzondere wetten anders is bepaald, heeft elke persoon het recht om kosteloos rectificatie te verkrijgen van alle onjuiste gegevens die op hem betrekking hebben.*
> *Verzoeken tot gegevensaanpassing worden ingediend via de toegangskanalen bepaald door de federale dienstenintegrator en de gebruikers bedoeld in artikel 2, lid 10, a) tot g).*
> *Telkens wanneer een verzoek tot aanpassing wordt ingediend via de federale dienstenintegrator, onderzoekt de federale dienstenintegrator of de aanvrager en het verzoek voldoen aan de toepasselijke voorwaarden.*
>
> *§ 2. Elke persoon heeft het recht te weten welke overheden en welke instanties de voorbije twaalf maanden zijn gegevens via het netwerk hebben geraadpleegd of bijgewerkt, met uitzondering van de bestuurlijke en gerechtelijke autoriteiten, toezichts- of opsporingsdiensten, de federale politie, de lokale politie, het Permanent Comité voor Toezicht op de politiediensten, het Permanent Comité voor Toezicht op de inlichtingendiensten, evenals hun respectieve onderzoeksdiensten, het Coördinatieorgaan voor de dreigingsanalyse, de Staatsveiligheid, de Algemene Dienst Inlichting en Veiligheid en de Algemene Inspectie van de federale en lokale politie.*
> *De federale dienstenintegrator voorziet in passende technische middelen om de uitvoering van schriftelijke overeenkomsten zoals bedoeld in artikel 14 te waarborgen.*
>
> *§ 3. Onverminderd de verantwoordelijkheid van de verantwoordelijken voor de verwerking van databanken en authentieke bronnen, stelt de federale dienstenintegrator de technische middelen ter beschikking van de gebruikers bedoeld in artikel 2, lid 10, a) tot g), om de betrokkenen in staat te stellen hun rechten uit te oefenen zoals bedoeld in artikel 15 van Verordening (EU) 2016/679 van 27 april 2016 van het Europees Parlement en de Raad betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van*

*Richtlijn 95/46/EG, ten aanzien van de verantwoordelijken voor de verwerking van de gegevensbanken en authentieke bronnen*" (onderstreping toegevoegd door de Autoriteit)[48] .

101. Volgens de Autoriteit moet de reikwijdte van deze bepaling, waarvan het dispositief moet worden gewijzigd, **worden verduidelijkt**.

***b) Verband met de AVG, specifieke bepalingen van de Belgische wetgeving en Artikel 13 van de wet van 2012***

102. In dit opzicht moet allereerst, en rekening houdend met artikel 23 van de AVG, het dispositief van artikel 16 van de wet van 2012, zoals gewijzigd door het Wetsontwerp, in een afzonderlijk eerste lid uitdrukkelijk bepalen dat het **geen afbreuk doet aan de AVG en aan "bijzondere"** (en niet "speciale, in lijn met het commentaar van de Raad van State") **wetten, decreten of ordonnanties** (aangezien het Wetsontwerp beoogt ook van toepassing te kunnen zijn op deelentiteiten**), die de rechten van de betrokkenen regelen, binnen de grenzen toegestaan door de AVG en de LTD**.

103. Op deze manier wordt gewaarborgd dat de bepaling in het Wetsontwerp enerzijds niet kan worden gelezen als een beperking van de rechten die zijn vastgelegd in de AVG, en anderzijds ook geen impact kan hebben op de beperkingen van de rechten van betrokkenen die elders in de Belgische wetgeving zouden zijn vastgelegd (en dit, overeenkomstig de AVG of Richtlijn (EU) nr. 2016/680 van het Europees Parlement en de Raad van 27 april 2016 betreffende de *bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, en betreffende het vrije verkeer van die gegevens en tot intrekking van Kaderbesluit 2008/977/JBZ van de Raad*).

---

[48] Het huidige artikel 16 van de wet van 2012 luidt als volgt:

*"1. Elke persoon heeft het recht om kosteloos de verbetering te bekomen van alle onjuiste gegevens die op hem betrekking hebben.*

*Verzoeken tot aanpassing van gegevens worden ingediend via de toegangskanalen bepaald door de federale dienstenintegrator en de deelnemende overheidsdiensten.*

*Telkens wanneer een aanpassingsaanvraag wordt ingediend via de federale dienstenintegrator, gaat de federale dienstenintegrator na of de aanvrager en de aanvraag voldoen aan de voorwaarden die in de relevante regelbanken zijn vastgelegd.*

*§ 2 Eenieder heeft het recht te vernemen welke overheden, welke instanties of welke personen in de loop van de voorbije zes maanden zijn gegevens via het net hebben geraadpleegd of bijgewerkt, met uitzondering van de administratieve en gerechtelijke overheden of diensten belast met het toezicht op of het onderzoek naar dan wel de vervolging of bestraffing van strafbare feiten, de federale politie, het Vast Comité van Toezicht op de politiediensten en het Vast Comité van Toezicht op de Inlichtingenwerk alsmede hun respectieve onderzoeksdiensten, het Coördinatieorgaan voor de dreigingsanalyse, [?[1] de staatsveiligheidsdienst, de algemene inlichtingen- en veiligheidsdienst] en de algemene veiligheidsinspectie [?[1] en de Algemene Inspectie van de Federale en Lokale Politie.*
*De federale dienstintegrator zorgt voor de gepaste technische middelen om de uitvoering te verzekeren van de beslissingen van het overlegcomité in toepassing van artikel 14*".

104. In dit verband is de Autoriteit van mening dat, gezien het bovenstaande commentaar, **artikel 13 van de wet van 2012 kan en moet worden aangepast met het oog op de breedte van het begrip gebruiker**. Zoals gewijzigd door het Wetsontwerp, luidt dit als volgt: "Bij *gebrek aan andersluidende wettelijke of reglementaire bepalingen, kent de federale dienstenintegrator aan de gebruikers geen bijkomende rechten toe met betrekking tot de raadpleging, mededeling of enige andere verwerking van gegevens bovenop de andere toepasselijke wettelijke en reglementaire bepalingen*" (onderstreping toegevoegd door de Autoriteit). **De Autoriteit is van mening dat deze bepaling om twee redenen moet worden aangepast: met het oog op het feit dat de betrokkene voortaan een gebruiker kan zijn in de zin van het Wetsontwerp, en om de rechtsgrondslag voor de aan andere gebruikers verleende rechten en de grenzen van de rol van de integrator in dit verband te verduidelijken.**

105. Wat dit tweede punt betreft, **is deze bepaling belangrijk omdat** ze het effect van de beginselen van voorzienbaarheid en rechtmatigheid herhaalt door *mutatis mutandis* te specificeren dat **de federale dienstenintegrator alleen mag toestaan dat persoonsgegevens worden verwerkt als het toepasselijke normatieve kader dat toestaat.**

106. De Autoriteit wijst er ook op dat artikel 13 **niet kan toestaan dat een regelgevende bepaling afwijkt van het beginsel dat ze vastlegt**, tenzij ze in strijd is met de beginselen van voorzienbaarheid en rechtmatigheid (die zijn vastgelegd in hogere normen, de Grondwet, het EVRM en het Handvest). De wet van 2012 kan immers niet indirect regelgevende bepalingen valideren die de federale dienstenintegrator de mogelijkheid zouden geven om gebruikers rechten inzake gegevensverwerking toe te kennen die niet reeds zijn voorzien door een norm met de status van wet (in overeenstemming met de beginselen van voorzienbaarheid en rechtmatigheid). **Artikel 13 moet dus worden aangepast en de verwijzing naar de regelgevende norm moet worden geschrapt**.

107. Pro memori heeft de Autoriteit de aanvrager ondervraagd over de vraag of dergelijke wettelijke of bestuursrechtelijke bepalingen momenteel bestaan. De aanvrager antwoordde: "*Nee, maar we kunnen niet uitsluiten dat er in de toekomst nieuwe regelgeving kan worden toegevoegd*". De Autoriteit merkt op dat dergelijke toekomstige regelgeving in ieder geval moet voldoen aan de beginselen van voorzienbaarheid en rechtmatigheid (en bijgevolg de essentiële elementen van de betreffende gegevensverwerkingen moet vastleggen).

108. Wat het eerste punt betreft, met betrekking tot de federale dienstenintegrator en de diensten die hij aanbiedt, aangezien het Wetsontwerp betrekking heeft op de transparantie en de **rechten van de betrokkenen**, moet dit **in principe een toegevoegde waarde hebben**. **Bepalingen die louter de toepassing herhalen van regels die reeds elders van toepassing zijn (zoals de AVG),**

**moeten uit het Wetsontwerp worden weggelaten**. Met andere woorden, op grond van het Wetsontwerp zelf (een wettelijke bepaling) wordt de betrokkene verondersteld aanvullende rechten te genieten.

***c) Verband met de taken van de federale dienstenintegrator***

109. **Vervolgens** moet het dispositief van de Wetsontwerp worden **verduidelijkt, rekening houdend enerzijds met de taken van de federale dienstenintegrator, en anderzijds de betrokken gebruikers**. Feitelijk brengt de uitbreiding van de gebruikers en taken van de federale dienstenintegrator een **herziening van het huidige artikel 16 van de wet van 2012** met zich mee, dat enkel van toepassing was op de uitwisseling van gegevens uit authentieke en niet-authentieke bronnen tussen deelnemende overheidsdiensten. Het Wetsontwerp moet duidelijk beschrijven, **met betrekking tot elk van deze taken ,het effect (de wettelijke toegevoegde waarde) van artikel 16 van de wet van 2012**, in die zin dat het voorziet in de tussenkomst van de federale dienstenintegrator, waar een dergelijk effect van het dispositief van het Wetsontwerp gewenst is. Zoals de Autoriteit net heeft opgemerkt, zou de bepaling in het Wetsontwerp niet nuttig zijn als ze louter de toepassing herhaalt van bepalingen die elders van toepassing zijn.

***d) Commentaar op de drie doelstellingen van de wetsontwerpbepaling***

110. De Autoriteit begrijpt dat de wetsontwerpbepaling **drie hoofddoelstellingen heeft,** waarop de volgende opmerkingen van toepassing zijn.

111. **Artikel 16, § 1**. Ten eerste gaat het erom de betrokkene in staat de stellen **de gegevens** op **zijn** verzoek te kunnen **rectificeren** (**§ 1**). Met betrekking tot deze doelstelling vereist het dispositief in voorbereiding de volgende opmerkingen.

112. De leden 2 en 3 van paragraaf 1 van artikel 16 van het Wetsontwerp moeten worden verduidelijkt in die zin dat een mogelijkheid wordt geboden om een verzoek tot rectificatie van gegevens die door bepaalde gebruikers worden verwerkt (die zijn bedoeld in artikel 2, lid 10, a) tot g)), kan worden ingediend **bij de federale dienstenintegrator zelf, waarbij deze laatste** in voorkomend geval **verantwoordelijk is** voor het doorsturen van het verzoek "*via de toegangskanalen*" *die* hijzelf en de gebruikers (bedoeld in lid 2) hebben *bepaald. De* essentiële toegevoegde waarde van een dergelijke bepaling is dat zij de betrokkene in staat stelt **contact op te nemen met één centraal aanspreekpunt** (verantwoordelijke voor de verwerking), die in staat is na te gaan waar de betrokken gegevens vandaan komen en welke andere gebruikers ze via zijn of haar diensten verwerken. Lid 3 van het dispositief in voorbereiding lijkt deze bedoeling te weerspiegelen, maar de interactie ervan met lid 2 is onduidelijk.

113. Daarnaast is de derde alinea van paragraaf 1 van artikel 16 van de wet van 2012 in voorbereiding onduidelijk, aangezien hierin wordt bepaald dat voor elke aanvraag om gegevens "aan te passen", "*de federale dienstenintegrator onderzoekt of de aanvrager en de aanvraag aan de toepasselijke voorwaarden voldoen*" (onderstreping toegevoegd door de Autoriteit). **Het dispositief moet verduidelijken welke rol de federale dienstenintegrator speelt met betrekking tot de verzoeken die hij ontvangt**. Is zijn rol bijvoorbeeld beperkt tot het verifiëren van de identiteit van de betrokkene? In dit verband moet worden benadrukt ***dat de* rol** (de bevoegdheid) **om te beslissen over het verzoek van de betrokkene** (om de betrokken gegevens al dan niet te wijzigen) *uiteindelijk* **moet toekomen aan de verantwoordelijke voor de verwerking van de gegevensbron**, tenzij het project de dienstenintegrator in dit opzicht een overheersende rol wil geven (maar om welke reden?).

114. **Artikel 16, § 2**: het doel van **paragraaf 2 is** de betrokkene in staat te stellen **centraal**, via de federale dienstenintegrator, te **bepalen welke entiteiten met zijn of haar gegevens hebben gewerkt** via de diensten van de federale dienstenintegrator. Meer specifiek worden de raadplegingen of updates "*via het netwerk*"[49] bedoeld.

115. De Autoriteit heeft de aanvrager gevraagd waarom in paragraaf 2 van voornoemd artikel 16 niet langer werd verwezen naar "*personen*" die toegang hadden gehad tot de gegevens, maar alleen naar "*autoriteiten*" of "*organisaties"*, zonder bovendien de begrippen gebruikers en dienstenintegratoren te gebruiken. Aanvrager antwoordde als volgt:

> *" De openbaarmaking van de identiteit van individuen (bijvoorbeeld medewerkers van de FOD's) die toegang hebben gehad tot de betreffende gegevens via de diensten van de federale dienstenintegrator, voor zover de federale dienstenintegrator al over deze informatie beschikt (in sommige gevallen vergemakkelijkt de federale dienstenintegrator de communicatie tussen de gegevensbron en de raadplegende entiteit, die zelf het beheer van gebruikers en toegangen verzorgt, zodat de raadplegende entiteit de identiteit van het individu kent en niet de federale dienstenintegrator), kan strijdig zijn met de rechten en vrijheden van deze personen. De mate waarin de identiteit van deze personen kan of moet worden bekendgemaakt, bijvoorbeeld op basis van het recht van toegang van de betrokkene wiens gegevens zijn geraadpleegd, moet worden beoordeeld in het licht van de beginselen van de algemene verordening gegevensbescherming en zal een beslissing van de verwerkingsverantwoordelijke vereisen die de gegevens heeft ontvangen of geraadpleegd.*

[49] Artikel 2, lid 8, van de wet van 2012 zoals gewijzigd door het Wetsontwerp definieert het netwerk als volgt:
*"alle databases, authentieke bronnen, computersystemen en netwerkverbindingen van gebruikers en de federale dienstenintegrator die onderling verbonden zijn via de federale dienstenintegrator*".

*Uw opmerking over het gebruik van het begrip gebruikers lijkt ons correct. De woorden "welke autoriteiten en welke organisaties" moeten* ***logischerwijs worden vervangen door "gebruikers als bedoeld in artikel 2, lid 10, onder a) tot en met g)"***" (vetgedrukt door de Autoriteit).

116. De Autoriteit neemt nota van deze toelichting en van het feit dat **de woorden *"autoriteiten*" en "*organisaties*" zullen worden vervangen door het woord *"gebruikers*"**. De Autoriteit wijst erop dat de betrokkene het recht heeft om de identiteit te verkrijgen van de ontvangers die de hem of haar betreffende persoonsgegevens hebben geraadpleegd (of gewijzigd in dit geval). Met andere woorden, **de dienstenintegrator zal[50] de verantwoordelijken voor de verwerking van de gegevens moeten identificeren**, dat wil zeggen, afhankelijk van concrete situaties, een overheidsinstantie, een specifieke afdeling van een overheidsinstantie, of zelfs in bepaalde gevallen een natuurlijke persoon[51] , een private entiteit die belast is met een openbare taak, enzovoort. Toegang tot de **identiteit van de natuurlijke personen** die door deze verwerkingsverantwoordelijken daadwerkelijk toegang hebben gehad tot de betreffende gegevens, vormt inderdaad een complexere kwestie die hier niet hoeft te worden uiteengezet[52] .

117. Hoewel de Autoriteit de vooruitgang opmerkt die het Wetsontwerp met zich meebrengt, waarbij nu informatie tot 12 maanden terug wordt gecommuniceerd in plaats van de huidige periode van 6 maanden zoals vastgelegd in artikel 12 van de wet van 2012, wijst de Autoriteit de aanvrager erop dat aangezien de federale dienstenintegrator **verantwoordelijk is voor de verwerking van de gegevens die nodig zijn voor de uitoefening van zijn taken, de AVG hem verplicht om op verzoek van de betrokkene de identiteit van de ontvangers die toegang hebben gehad tot de gegevens te communiceren, zonder een specifieke periode vast te stellen.**

118. De Autoriteit is van mening dat **een periode van 12 maanden te kort is**. Toen de aanvrager werd gevraagd welke criteria werden gehanteerd om een dergelijke periode te bepalen, heeft hij geen nadere toelichting gegeven. De Autoriteit herinnert eraan dat artikel 12, lid 5, van de AVG de situatie regelt waarin de betrokkene aan de verwerkingsverantwoordelijke verzoeken zou richten die kennelijk ongegrond of buitensporig zijn. En zij is van mening dat de vraag over welke periode de betrokkene toegang kan krijgen tot de identiteit van de gegevensontvangers **in verband moet worden gebracht met de periode die door de verwerkingsverantwoordelijke moet worden gedekt in het kader van de te implementeren audit trail,** overeenkomstig de beginselen van beveiliging van de verwerking (het instellen van technische en organisatorische maatregelen, artikel 32 van de

[50] Zie bijvoorbeeld C.J.U.E. (1e Kamer), arrest van 12 januari 2023, *RW tegen Österreichische Post AG*, zaak C-154/21.

[51] De Autoriteit heeft bijvoorbeeld al overwogen dat een onderzoeker of een magistraat voor de verwerking verantwoordelijken kunnen zijn.

[52] Zie bijvoorbeeld C.J.U.E. (1e Kamer), arrest van 22 juni 2023, *J.M.*, zaak C-579/21, overweging 73 e.v.

AVG) en de verantwoordelijkheid van de verwerkingsverantwoordelijke (artikel 24 van de AVG). **Zolang de verwerkingsverantwoordelijke over deze informatie beschikt, moet de betrokkene er toegang toe hebben.** In dit geval gaat het om een periode van **10 jaar.**

119. Ten slotte, met betrekking tot **de uitzondering** voorzien in het Wetsontwerp, aangezien de federale dienstenintegrator een verantwoordelijke voor de verwerking is, kan **de informatie over de mededeling van de gegevens** aan "*bestuurlijke en gerechtelijke overheden of diensten belast met het toezicht of het onderzoek of de vervolging of de repressie van misdrijven, de federale politie, de lokale politie, het Vast Comité van Toezicht op de politiediensten en het Vast Comité van Toezicht op de inlichtingendiensten en hun respectieve onderzoeksdiensten, het Coördinatieorgaan voor de dreigingsanalyse, de Veiligheid van de Staat, de Algemene Inlichtingen- en Veiligheidsdienst en de Algemene Inspectiedienst van de Federale Politie en de Lokale Politie*", **mag enkel worden weggelaten indien, en enkel indien, *in concreto,* krachtens de toepasselijke wetgeving niet daadwerkelijk kan worden meegedeeld**. Dit vereist dat de federale dienstenintegrator *a priori de* technische en organisatorische maatregelen evalueert en invoert die hem in staat stellen om te bepalen welke verwerkingen al dan niet onder de uitzondering vallen. Het **dispositief in voorbereiding moet dus op dit punt worden aangepast**.

120. **Artikel 16, § 3** Tot slot verplicht **paragraaf 3** van het dispositief in voorbereiding de federale dienstenintegrator om **gebruikers een technische voorziening te bieden waarmee betrokkenen hun recht op toegang kunnen uitoefenen**. De memorie van toelichting bij paragraaf 3 van voornoemde bepaling luidt als volgt:

> "*Paragraaf 3 bepaalt dat de dienstenintegrator de technische middelen ter beschikking moet stellen die burgers in staat stellen om, met betrekking tot authentieke bronnen, hun recht op toegang als bedoeld in artikel 15 van de AVG uit te oefenen. Dit is natuurlijk alleen mogelijk als de betrokkene dit recht heeft. Dit ontslaat de verantwoordelijken voor gegevensbronnen en authentieke bronnen niet van hun verplichtingen en verantwoordelijkheid in dit opzicht*" (onderstreping toegevoegd door de Autoriteit).

121. Ten eerste merkt de Autoriteit op dat **de memorie van toelichting in overeenstemming moet worden gebracht met het dispositief van het Wetsontwerp,** aangezien **paragraaf** 3 van artikel 16 van de wet van 2012 in voorbereiding niet alleen van toepassing is op authentieke gegevensbronnen, maar **ook op databanken die geen authentieke gegevensbronnen zijn**.

122. Vervolgens wijst het erop dat dit een **volwaardige taak is van de federale dienstenintegrator**. Dit zou dus ook moeten worden voorzien door **artikel 4 van de wet van 2012 in voorbereiding**.

**II.7. Diverse punten**

**II.7.1. Gegevensbeveiliging**

123. Met betrekking tot gegevensbeveiliging voorziet artikel 14 van de wet van 2012 zoals gewijzigd door het Wetsontwerp: "*Voor elke uitwisseling van gegevens via de federale dienstenintegrator wordt het volgende vastgelegd tussen de gebruiker bedoeld in artikel 2, lid 10, a) tot g), en de federale dienstenintegrator*" (onderstreping toegevoegd door de Autoriteit): D.w.z. in het bijzonder wie welke identiteitsauthenticatie, -verificaties en -controles uitvoert, en de "*wijze waarop wordt verzekerd dat een volledige reconstructie kan plaatsvinden in geval van een onderzoek, op initiatief van een betrokken toezichthoudende autoriteit of orgaan of naar aanleiding van een klacht, van welke natuurlijke persoon wanneer en voor welk doel gebruik heeft gemaakt van welke dienst met betrekking tot welke persoon*".

124. De Autoriteit vroeg de aanvrager naar **de verdeling van de verantwoordelijkheden tussen de dienstenintegrator en de gebruiker voor dit doel** (wie moet wat registreren en wie moet bepalen wat moet worden geregistreerd). De aanvrager antwoordde als volgt: "*Het lijkt onmogelijk om dit van tevoren te bepalen. Het is een **gezamenlijke verplichting** om ervoor te zorgen dat de nodige afspraken worden gemaakt overeenkomstig de rol en verantwoordelijkheid van elke partij in de uitwisseling. Deze regelingen zijn opgenomen in de gebruikersovereenkomst*" (vetgedrukt door de Autoriteit).

125. De Autoriteit begrijpt daarom dat de verplichtingen die zijn vastgelegd in artikel 14 van de wet van 2012, zoals gewijzigd door het Wetsontwerp, voor zover ze betrekking hebben op de verwerking van persoonsgegevens, **de gezamenlijke verantwoordelijkheid zijn van de federale dienstenintegrator en de betrokken gebruiker**[53] .

126. Meer in het algemeen kan de wijziging van sectie 14 van de wet van 2012 niet worden beperkt tot lid 1, tenzij deze bepaling haar samenhang verliest. Eerst en vooral is de Autoriteit van mening dat alinea 1 van artikel 14 van de wet van 2012 **opnieuw moet worden geformuleerd om duidelijk te maken dat de verplichtingen op de gebruiker en de dienstenintegrator rusten**.

127. En vervolgens moet het even duidelijk en algemeen aangeven dat, **in overeenstemming met de van toepassing zijnde wetgeving betreffende de gegevensuitwisseling**, de gebruiker en de integrator **bepalen en/of opnemen** (indien de toepasselijke wetgeving al regels op dit gebied bevat) **in de gebruiksvoorwaarden zoals bedoeld in artikel 5, § 2**, de vermelde elementen. De toepasselijke wetgeving betreffende de gegevensuitwisseling kan immers relevante regels op dit

[53] Zie hierover de overwegingen nrs. 85-88.

gebied bevatten en bovendien moet de "wijze van raadpleging van gegevens" zoals bedoeld in lid 5 van artikel 14, zonder afbreuk te doen aan met name het recht op toegang van de betrokken personen.

128. Daarnaast moeten sommige concepten of passages van artikel 14 zoals gewijzigd door het Wetsontwerp **worden herschreven om duidelijker te zijn**. Zo moet het zich niet langer richten op "instanties", maar op de in wet opgenomen begrippen (gebruiker, dienstenintegrator). Bovendien gaat het er niet om hoe "men" ervoor zorgt dat een volledige reconstructie kan plaatsvinden, maar wel hoe "de federale dienstenintegrator en de gebruiker ervoor zorgen" dat een dergelijke reconstructie mogelijk is.

129. Tot slot **benadrukt de Autoriteit het belang van de termijn van minimaal 10 jaar** die is vastgelegd in artikel 14, lid 5, van de wet van 2012 in voorbereiding, die al van kracht is en niet ter discussie wordt gesteld in het Wetsontwerp. Gezien de taken van de federale dienstenintegrator is het essentieel dat een *audit trail* (met inbegrip van de bijbehorende *logging*) van een verwerkingsoperatie over een periode van 10 jaar kan worden gereconstrueerd.

### II.7.2. Bevoegdheden van de Koning krachtens artikel 44 van de wet van 2012

130. Artikel 44 van de wet van 2012, zoals gewijzigd door het Wetsontwerp (waarbij de termen "*deelnemende overheidsdiensten*" worden vervangen door de termen "*gebruikers*") bepaalt: "*De Koning kan, bij een in ministerraad overlegd besluit, de taken van de in hoofdstuk 5 bedoelde organen regelen, alsook de latere modaliteiten van de samenwerking tussen de federale dienstenintegrator en de gebruikers*". De Autoriteit heeft de aanvrager ondervraagd om na te gaan of de in artikel 44 van de wet van 2012 aan de Koning toegekende bevoegdheid een impact zou kunnen hebben op de verwerking van persoonsgegevens door de dienstenintegrator en de gebruikers. De aanvrager antwoordde als volgt:

> "Tot op heden is er *geen Koninklijk Besluit uitgevaardigd uit hoofde van artikel 44. Een Koninklijk Besluit op grond van artikel 44 dat gevolgen zou kunnen hebben voor de verwerking van persoonsgegevens zou in ieder geval alleen mogelijk zijn in het kader van de delegatie in kwestie,* ***waarin in dit geval niet is voorzien***" (vetgedrukt toegevoegd door de Autoriteit).

131. De Autoriteit neemt kennis van dit antwoord en is van mening dat **in de memorie van toelichting bij het Wetsontwerp moet worden benadrukt dat artikel 44 van de wet van 2012, dat door dit artikel wordt gewijzigd, niet tot doel heeft een bevoegdheid betreffende de verwerking van persoonsgegevens aan de Koning te delegeren** . De Autoriteit benadrukt dat een dergelijke bepaling niet beantwoordt aan de vereisten van voorzienbaarheid en rechtmatigheid die reeds elders werden vermeld, en bijgevolg niet de basis kan vormen voor de bevoegdheid van de Koning om

besluiten uit te vaardigen die een impact hebben op de verwerking van persoonsgegevens door de federale dienstenintegrator of zijn gebruikers.

### II.7.3. Adviseur informatiebeveiliging

132. De Autoriteit heeft de aanvrager ondervraagd over de reden waarom het Wetsontwerp **artikel 22, lid 2, van de wet van 2012 schrapt**, waarin staat: *"De veiligheidsadviseur aangesteld door de federale dienstenintegrator zal, naast de eerder genoemde functies in lid 1, belast zijn met bewustmakingsactiviteiten met betrekking tot de beveiliging van de informatie van de deelnemende openbare diensten."* De aanvrager antwoordde als volg:

> "*De inclusie van de bewustmakingsmissie van de veiligheidsadviseur van de federale dienstenintegrator met betrekking tot de informatiebeveiliging van de (toenmalige) deelnemende overheidsdiensten in de wet van 2012 dateert natuurlijk van vóór de inwerkingtreding van de AVG. Sindsdien is het de verantwoordelijkheid van elke gebruiker om een eigen Functionaris voor gegevensbescherming (Data Protection Officer - DPO) aan te stellen, die verantwoordelijk is voor de bewustmaking binnen de eigen organisatie. Deze missie en verantwoordelijkheid behoren niet tot de federale dienstenintegrator. We willen natuurlijk vermijden dat deze wet wordt gebruikt als een middel om verantwoordelijkheid te ontlopen*.

133. **De Autoriteit neemt nota van de schrapping van** de bepaling in kwestie en de redenering erachter. Zij wijst erop dat als deze bepaling zou worden gehandhaafd, dit de voor de verwerking verantwoordelijken en de functionarissen voor gegevensbescherming geenszins zou ontslaan van hun verplichtingen uit hoofde van de AVG.

134. Bovendien bepaalt artikel 20, lid 2, van de wet van 2012, zoals gewijzigd door het Wetsontwerp, , het volgende: "*Een informatiebeveiligingsadviseur kan de functie van functionaris voor gegevensbescherming uitoefenen in overeenstemming met de vereisten zoals vermeld in artikel 38, lid 6, van de AVG*". Deze adviseur valt "onder de directe autoriteit van de leidinggevende van de gebruiker of de federale dienstenintegrator", zoals bepaald in artikel 21 van de wet van 2012, zoals gewijzigd door het Wetsontwerp.

135. In dit verband vraagt de Autoriteit zich af of de combinatie van de rollen van informatiebeveiligingsadviseur en Functionaris voor Gegevensbescherming zoals toegestaan door het Wetsontwerp, verenigbaar is met de AVG. Hoewel artikel 38, lid 6, van de AVG bepaalt dat de Functionaris voor Gegevensbescherming "andere taken en werkzaamheden kan verrichten" dan die welke hij vaststelt, maar alleen op voorwaarde dat de "verwerkingsverantwoordelijke of de verwerker

ervoor zorgt dat deze taken en werkzaamheden geen belangenconflict veroorzaken." In dit geval rijst de vraag naar het bestaan van een belangenconflict, aangezien het Wetsontwerp voorziet in de advisering door de veiligheidsadviseur op het gebied van informatiebeveiliging, met bijzondere aandacht voor gegevens- en netwerkbeveiliging, en het uitvoeren van opdrachten op het gebied van informatiebeveiliging. Deze activiteiten zijn gerelateerd aan het bepalen van de middelen en (sub-)doeleinden van de verwerking van persoonsgegevens met betrekking tot informatiebeveiliging, zodat het toewijzen van deze aanvullende rol aan de Functionaris voor Gegevensbescherming naar alle waarschijnlijkheid een belangenconflict met zich meebrengt[54] .

136. Op deze vraag antwoordde de aanvrager als volgt:

> *"Dit artikel vermeldt alleen de mogelijkheid van combinatie onder verwijzing naar artikel 38, paragraaf 6, waarin staat dat de verwerkingsverantwoordelijke (of de verwerker) ervoor moet zorgen dat de taken en werkzaamheden van de FG geen belangenconflict veroorzaken. Wat betreft de cumulatieve voorwaarden moeten alle betrokken partijen uiteraard rekening houden met de beslissingen van de APG hieromtrent (zie https://www.gegevensbeschermingsautoriteit.be/professioneel/avg/de-functionaris-voor-gegevensbescherming/aanwijzing).*

137. Artikel 20, lid 2 van de wet van 2012 zoals geformuleerd in het Wetsontwerp wekt niettemin de indruk dat de cumulatie *a priori* geen aanleiding zal geven tot belangenconflicten, terwijl, zoals zojuist vermeld, een dergelijk belangenconflict zich waarschijnlijk wel zal voordoen. Voor het overige heeft de bepaling in het Wetsontwerp geen juridische meerwaarde om de voorgestelde combinatie toe te staan, op voorwaarde dat de AVG wordt nageleefd: indien de AVG hier niet tegen is, kan de verwerkingsverantwoordelijke zelf een cumulatieve benoeming doen (zonder specifieke toestemming van het Belgische recht); indien de AVG hiertegen is, kunnen noch het Belgische recht, noch de verwerkingsverantwoordelijke een dergelijke benoeming toestaan. **In deze context is de Autoriteit van mening dat het tweede lid 2 van artikel 20 moet worden geschrapt**.

138. Ten slotte bepaalt artikel 20 in het Wetsontwerp dat niet alleen de dienstenintegrator, maar ook alle gebruikers zoals bedoeld in artikel 2, lid 10, a) tot g) een veiligheidsadviseur moeten aanstellen. **Dit betekent dus dat deze vereiste ook van toepassing kan zijn op natuurlijke personen**. In dit verband is de Autoriteit van mening dat de aanvrager **duidelijk moet maken in welke gevallen**

[54] Voor een weliswaar andere zaak, maar waarin de beginselen worden herhaald, zie het besluit van de Litigation Division van de Autoriteit nr. 141/2021 van 16 december 2021, beschikbaar op

https://www.gegevensbeschermingsautoriteit.be/publications/beslissing-ten-gronde-nr.-141-2021.pdf, laatst geraadpleegd op 24/01/2023, overwegingen 59 e.v.

**het niet verplicht is om een veiligheidsadviseur aan te stellen, indien van toepassing door te verwijzen naar natuurlijke personen in de te bepalen gevallen.**

### II.7.4. Uitbreiding naar Gemeenschappen en Gewesten

139. Het Wetsontwerp voegt een nieuw artikel *46bis* toe aan de wet van 2012, dat als volgt luidt:

> *"Onder de voorwaarden en volgens de modaliteiten bepaald door de Gemeenschappen en de Gewesten en in overleg met de federale dienstenintegrator, kunnen de Gewesten, Gemeenschappen, lokale overheden en de daarvan afhankelijke organisaties een beroep doen op de diensten van de federale dienstenintegrator*" (onderstreping toegevoegd door de Autoriteit).

140. De Autoriteit heeft de aanvrager ondervraagd over de reden waarom er niet voorzien is in een samenwerkingsovereenkomst voor dit doel. Zij heeft hem ook ondervraagd over wat er bedoeld wordt met "overleg" met de federale dienstenintegrator. De aanvrager antwoordde als volgt:

> "*De beoogde samenwerking tussen de betrokken partijen* ***wordt geregeld door het Samenwerkingsakkoord van 26 augustus 2013*** *tussen de federale, gewestelijke en gemeenschapsoverheden voor het harmoniseren en uitlijnen van de initiatieven die de realisatie van een geïntegreerd e-government beogen (Belgisch Staatsblad (fgov.be))* ***Het overleg maakt uiteraard deel uit van de uitwerking van dit samenwerkingsakkoord*** *en heeft betrekking op de operationele modaliteiten van de samenwerking*" (vetgedrukt door de Autoriteit).

141. **Eerst en vooral verwijst** de Autoriteit **op dit punt naar de opmerkingen van de Raad van State over de bepaling in het Wetsontwerp[55]** . Aangezien de door de aanvrager bedoelde

[55] In het bijzonder stelt de Raad van State het volgende:

*"De reikwijdte van de aldus aan de gewesten, gemeenschappen, lokale overheden en hun afhankelijke organen verleende machtiging is niet duidelijk.*

***Indien het er enkel om gaat deze entiteiten toegang te verlenen tot de gegevens die door de federale dienstenintegrator worden verwerkt door middel van de creatie van een daartoe strekkende wettelijke machtiging door de gemeenschappen en gewesten, levert de bepaling geen moeilijkheden op [...]***.

***Indien het, meer in het algemeen, gaat om het*** *machtigen van de entiteiten in kwestie om gebruik te maken van de diensten van de federale dienstenintegrator in het licht van al zijn taken zoals gespecificeerd door artikel 4 van het wetsontwerp van 15 augustus 2012, om deze te belasten met de uitvoering van hun eigen beleid (zoals de ontwikkeling van IT-oplossingen in het kader van de uitoefening van hun eigen bevoegdheden), vereist een dergelijke machtiging dat een beroep wordt gedaan op een samenwerkingsmechanisme in de zin van de artikelen 92bis of 92bis/1 van de bijzondere wet van 8 augustus 1980 betreffende de institutionele hervormingen. (verwijzingen weggelaten door de Autoriteit).*

*Door middel van een samenwerkingsovereenkomst kunnen de betrokken autoriteiten niet alleen besluiten om een gezamenlijke instelling op te richten, maar kunnen ze er ook voor kiezen om gebruik te maken van de diensten en instellingen van andere autoriteiten. In dit geval moet de autoriteit die de diensten en instellingen aanbiedt echter zelf materieel en territoriaal bevoegd zijn en moeten de partijen het beginsel van financieel federalisme respecteren .*

[...]

samenwerkingsovereenkomst al bestaat, kon het in artikel *46 bis* bedoelde overleg in het kader van de opstelling ervan niet plaatsvinden. De Autoriteit benadrukt nogmaals dat het samenwerkingsakkoord waarnaar de aanvrager verwijst, niet specifiek handelt over de relatie tussen de federale dienstenintegrator en de deelentiteiten en de van hun afhankelijke overheden[56] . Het Wetsontwerp moet verduidelijken hoe het de deelentiteiten en hun afhankelijke overheden in staat wil stellen om gebruik te maken van de diensten van de federale dienstenintegrator.

**Conclusie**

**Om deze redenen,**
**De Autoriteit is van mening dat**

**1.** Het Wetsontwerp vereist een effectbeoordeling met betrekking tot de gegevensbescherming en het is voorbarig om uitspraken te doen over bepalingen van de Europese wetgeving die nog niet definitief zijn (**overwegingen 8-11**) ;

**2**. Indien de aanvrager heeft afgezien van het wijzigen van het begrip van een authentieke gegevensbron zoals vastgelegd in de wet van 2012 in het kader van de voorbereiding van het Wetsontwerp, roept het Wetsontwerp zoals voorgelegd aan de Autoriteit niettemin toch enkele opmerkingen op. Bovendien moet het Wetsontwerp een duidelijk onderscheid maken tussen de uitwisseling van gegevens die afkomstig zijn uit authentieke bronnen en de uitwisseling van gegevens die niet afkomstig zijn uit authentieke bronnen (**overwegingen 12-22**) ;

**3.** Wat betreft de benoeming van authentieke gegevensbronnen, moet het Wetsontwerp het beginsel van positief recht handhaven waarbij een Koninklijk Besluit, besproken in de ministerraad, vereist is, eerder dan een beslissing van het Coördinatiecomité. Het Wetsontwerp voegt waarde toe op het gebied van gegevensbescherming door in de wet de criteria voor de benoeming van authentieke bronnen vast te leggen, criteria die verfijnd moeten worden (**overwegingen 23-32**).

---

***Zonder zich uit te spreken over de inhoud van dit samenwerkingsakkoord, stelt de afdeling Wetgeving vast dat het niet het voorwerp heeft uitgemaakt van een bekrachtiging door de wetgever, hoewel*** *een dergelijke bekrachtiging op grond van artikel 92bis, § 1, tweede lid, van de bijzondere wet van 8 augustus 1980 vereist was. Het gevolg is dat het samenwerkingsakkoord momenteel geen effect heeft krachtens voornoemde bepaling. Bijgevolg is de ontwerpbepaling niet verder onderzocht*" (onderstreping toegevoegd door de Autoriteit).

[56] Naar de integratoren wordt verwezen in de artikelen 3, lid 6 en 5, lid 5 van het samenwerkingsakkoord. De enige verwijzing naar de federale dienstenintegrator staat in de "gemeenschappelijke acties", in artikel 5, lid 5, van het samenwerkingsakkoord, dat bepaalt dat om de doelstelling bedoeld in artikel 1er van het akkoord en de onderdelen bedoeld in artikel 4 te bereiken, de partijen zich ertoe verbinden om, overeenkomstig hun respectieve bevoegdheden, "*deel te nemen aan het overlegcomité voor dienstenintegratoren voorzien in de wet van 15 augustus 2012 betreffende de oprichting en de organisatie van een federale dienstenintegrator*". Artikel 3, lid 6 voorziet in het principe van "*constructieve samenwerking en duidelijke afspraken tussen bestaande en toekomstige dienstenintegratoren*".

**4.** Met betrekking tot de gebruikers in de zin van het Wetsontwerp moet de definitie zoals bedoeld in artikel 10, lid 2, van de wet van 2012 zoals gewijzigd door het Wetsontwerp worden aangepast om consistentie te waarborgen, en artikel 46 van het Wetsontwerp moet worden aangepast om enerzijds de reikwijdte te hebben die door de aanvrager wordt erkend, en anderzijds om in overeenstemming te zijn met de beginselen van voorzienbaarheid en rechtmatigheid (**overwegingen 33-42**) ;

**5.** Met betrekking tot de taken van de federale dienstenintegrator moet het eerste lid van artikel 4 van de wet van 2012 worden aangepast, rekening houdend met name met de nieuwe taken van de integrator. Het dispositief van het Wetsontwerp moet duidelijk verwijzen naar de relevante bepalingen van de Europese wetgeving die het beoogt aan te vullen of uit te voeren. De verschillende taken van de federale dienstenintegrator moeten duidelijk worden onderscheiden in het Wetsontwerp. Het Wetsontwerp moet de verwerkingen definiëren die mogelijk worden gemaakt door herbruikbare toepassingen en verduidelijken of deze beschikbaar kunnen worden gesteld in de vorm van diensten. Artikel 4, lid 12, van de wet van 2012 zoals gewijzigd door het Wetsontwerp lijkt geen juridische meerwaarde te hebben. De Autoriteit neemt kennis van de intentie van de aanvrager om de verwijzing naar de "G-Cloud" in de considerans te schrappen (**overwegingen 43-68**) ;

**6.** De Autoriteit is van mening dat het Wetsontwerp de reikwijdte van de regel, volgens welke de dienstenintegrator zijn diensten met toestemming van de gebruiker aanbiedt, ook met betrekking tot de nieuwe taken van de integrator, moet uitbreiden. Het Wetsontwerp moet duidelijk identificeren wat de vrijheid van de gebruiker is, met name met betrekking tot de toegang tot gegevens die beschikbaar zijn via de diensten van de integrator (**overwegingen 69-79**) ;

**7.** Wat betreft de vaststelling van verantwoordelijkheden met betrekking tot gegevensverwerking, sluit het Wetsontwerp direct aan bij de praktijk van de adviezen van de Autoriteit, met dien verstande dat er gezamenlijke verantwoordelijkheden moeten worden geïdentificeerd met betrekking tot gegevensverwerking, met name met betrekking tot de uitwisseling van gegevens tussen overheidsinstanties via de diensten van de integrator. Artikel 15 van de wet van 2012 zoals gewijzigd door het Wetsontwerp moet ook worden aangepast om in overeenstemming te zijn met de beginselen van voorzienbaarheid en rechtmatigheid, waarbij artikel 6 van de wet van 2012 zoals gewijzigd door het Wetsontwerp zou moeten worden geschrapt. Artikel 14 van het Wetsontwerp moet de gevolgen verduidelijken van de beoordeling die moet worden uitgevoerd door de dienstenintegrator in geval van een verzoek om gegevens te raadplegen of te verstrekken, en de mogelijke rol van de gegevensbron (**overwegingen 80-91**) ;

**8.** De beslissingsbevoegdheid van het Coördinatiecomité moet worden verduidelijkt en in de memorie van toelichting bij het Wetsontwerp moet erop worden gewezen dat artikel 33 van de wet van 2012 niet tot doel heeft het Coördinatiecomité in staat te stellen bindende besluiten te nemen met betrekking tot de verwerking van persoonsgegevens (**overwegingen 92-93**) ;

**9.** Het Wetsontwerp voegt waarde toe op het gebied van gegevensbescherming door de transparantie in de werking van de dienstenintegrator te versterken. Het moet ook voorzien in communicatie in een apart register van niet-authentieke gegevensbronnen die toegankelijk zijn via de diensten van de integrator (**overwegingen 94-95**) .

**10.** Als het Wetsontwerp de dienstenintegrator kan vrijstellen van het sluiten van de protocollen zoals bedoeld in artikel 20 van de LTD, is de Autoriteit van mening dat dit onder de voorwaarde is dat de overeenkomsten die worden gesloten in het kader van de toegang tot de diensten van de integrator de elementen van de protocollen bevatten zoals bedoeld in de WVG en dat de relevante secties daarvan op zijn minst openbaar moeten worden gemaakt. De functionaris voor gegevensbescherming moet ook worden betrokken bij de opstelling van de overeenkomsten en gebruiksvoorwaarden (**overwegingen 94-99**) ;

**11.** Artikel 16 van de wet van 2012, zoals gewijzigd bij het Wetsontwerp, betreffende het recht van rectificatie en toegang van betrokkenen, moet worden aangepast. Er moet worden gespecificeerd dat dit artikel geen afbreuk doet aan de AVG en aan specifieke wetten, decreten of verordeningen die anderszins van toepassing zijn in het Belgische recht. Artikel 13 van de wet van 2012, zoals gewijzigd door het Wetsontwerp, moet worden aangepast gezien het feit dat de betrokken persoon een gebruiker kan zijn, en om te voldoen aan de beginselen van voorzienbaarheid en rechtmatigheid. Het Wetsontwerp moet de toepassing van het voornoemde artikel 16 nog verduidelijken in het licht van de verschillende taken van de dienstenintegrator.

Deze drie alinea's van deze bepaling vereisen enkele verduidelijkingen en preciseringen. Met name de voorziene uitzondering is te ruim en de communicatie van de identiteit van de gebruikers aan wie de gegevens door de federale dienstenintegrator worden doorgegeven, kan niet worden beperkt tot de 12 maanden die aan het verzoek voorafgaan, maar moet worden uitgebreid tot 10 jaar (**overwegingen 101-122**) ;

**12.** Wat betreft de gegevensbeveiliging moet artikel 14 van de wet van 2012, zoals gewijzigd door het Wetsontwerp worden aangepast, met name om te verduidelijken wie

verantwoordelijk is voor de verplichtingen die erin zijn vastgelegd (**overwegingen 123-129**) ;

**13.** De memorie van toelichting bij het Wetsontwerp moet benadrukken dat het doel van artikel 44 van de wet van 2012, dat het wijzigt, niet is om aan de Koning een bevoegdheid te delegeren betreffende de verwerking van persoonsgegevens (**overwegingen 130-131**) ;

**14.** De bepaling dat de informatiebeveiligingsadviseur ook als de functionaris voor gegevensbescherming kan worden benoemd, moet worden weggelaten en het Wetsontwerp moet voorzien in een uitzondering op de verplichting om een informatiebeveiligingsadviseur aan te stellen wanneer de betrokken gebruiker een natuurlijk persoon is (**overwegingen 132-138**) ;

**15.** Het Wetsontwerp moet verduidelijkt worden over de manier waarop het de deelentiteiten en de onder hun bevoegdheid vallende overheden in staat wil stellen om gebruik te maken van de diensten van de federale dienstenintegrator (**overwegingen 139-141**).

Voor het Kenniscentrum,
Cédrine Morlière, Directeur