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)
Mots-clés : source authentique (définition, désignation, critères, principes) – responsables (conjoints) du traitement – droits des personnes concernées (accès et rectification) – analyse d'impact (au stade du processus normatif) – intégrateur de service
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.***

[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.

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 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

[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.

l'article 2, 6°, de la loi de 2012 est modifié par l'article 2 du Projet. Le concept de « *donnée 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>*

- [3 ...]3;

*(- 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 responsables du traitement, 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, sans fixer de période particulière.**

118. L'Autorité est d'avis qu'une **période de 12 mois est trop courte**. 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 **doit être mise en relation avec la période que doit couvrir l'*audit trail* à mettre en place par le responsable du traitement[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, **aussi longtemps que le responsable du traitement dispose de cette information, la personne concernée doit pouvoir y avoir accès**. Il s'agit en l'occurrence d'une période de **10 ans**.

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,
(sé) Cédrine Morlière, Directrice