Mise en place d'une source authentique

Version 1 – Mars 2019

DG Transformation digitale du SPF BOSA

Federale overheidsdienst
Beleid en Ondersteuning
Service public fédéral
Stratégie et Appui

TABLE DES MATIÈRES

Aperçu

Ce document décrit les activités et points d'attention courants liés à la mise en place d'une source authentique. Les informations reprises dans le présent document visent à soutenir d'autres services publics et à accélérer la mise en place de sources authentiques.

Chaque source authentique est cependant unique en termes d'attentes, d'utilisation et de mise en place. Le propriétaire de la source reste responsable de l'exécution correcte des actions ainsi que de la définition d'actions supplémentaires afin de s'assurer du bon fonctionnement de la source, du respect de toutes les législations pertinentes et de la prise en compte des attentes des parties prenantes.

Vous trouverez à la section 5 des définitions et explications des termes utilisés.

1 Qu'est-ce qu'une source authentique ?

1.1 Le concept de « source authentique »

« Une source authentique est une banque de données dans laquelle sont conservées des données authentiques. Ces données font foi comme données uniques et originales concernant des personnes ou faits de droit. » (Loi relative à la création et à l'organisation d'un intégrateur de services fédéral, 15 août 2012, Art. 2).

Une source authentique est la référence par excellence pour obtenir des données déterminées. Elle offre des garanties spécifiques en termes *d'exactitude*, d'*exhaustivité* et de *disponibilité* de ces données.

- Exactitude: Les données demandées à partir d'une source authentique sont considérées comme correctes et à jour.
- Exhaustivité : la source authentique comprend la population entière de données.
- Disponibilité : la source authentique est consultable à une fréquence prédéfinie par les personnes disposant des autorisations correctes.

L'objectif d'une source authentique est de *simplifier* les obligations administratives des citoyens et personnes morales en garantissant que les données déjà disponibles pour l'Administration dans une source authentique ne doivent plus à nouveau être communiquées au service public fédéral.

Une source authentique joue donc un rôle central à différentes fins :

1. En principe, les personnes physiques et morales ne doivent *fournir qu'une fois* leurs données à la source authentique.
2. Une source authentique est ouverte à d'autres services publics afin qu'ils demandent ces données à cette source et ne se chargent *plus chacun distinctement* de la collecte des mêmes informations.

(Loi « Only Once », 5 mai 2014, Art. 2).

1.2 Quels sont les avantages d'une source authentique ?

Les sources authentiques présentent des avantages tant pour l'instance qui agit en tant que propriétaire de la source, que pour les utilisateurs des données authentiques ou encore pour les citoyens/entreprises.

1. Qualité accrue des données

Grâce aux *garanties et aux procédures*, la qualité des données dans une source authentique est déjà élevée. En outre, davantage de personnes utiliseront les mêmes données, ce qui permettra de détecter et de corriger plus rapidement des erreurs éventuelles afin de continuer à accroître la qualité des données.

2. Diminution du nombre de duplicatas

Les données ne doivent plus être dupliquées dans des banques de données locales auprès de différentes instances. Les services publics peuvent donc toujours disposer des *données les plus actuelles*.

3. Diminution des frais d'administration

En cas de modifications des données, il ne faut adapter *qu'une fois une seule source*. La gestion, la sécurisation et la maintenance des données ne doivent se faire qu'à un seul endroit.

4. Disponibilité garantie

Grâce aux garanties de disponibilité, tous les utilisateurs ont un *aperçu clair des périodes* pendant lesquelles ils ont accès aux données.

5. Saisie unique

Les citoyens et les entreprises ne doivent *fournir qu'une seule fois leurs données aux autorités*. Ces dernières sont ensuite obligées d'ouvrir et de réutiliser ces données.

6. Sécurité accrue

En désignant clairement les *personnes* dont le rôle est d'assumer la responsabilité en matière de sécurité (DPD et conseiller en sécurité) et en rédigeant des *procédures* pour le traitement, l'enregistrement et l'échange des données, il est possible d'accroître la sécurité et d'éviter un accès non autorisé aux données.

7. Accessibilité

Quand la source est reconnue comme authentique, elle est ajoutée à l'*aperçu sur le site web du SPF BOSA*. Tous les utilisateurs qui ont besoin de ces données pour leur propres finalités peuvent ainsi *facilement* retrouver le propriétaire et, si nécessaire, *demander une autorisation* d'*accès* à l'instance compétente.

2 Comment mettre en place une source authentique ?

2.1 Quelles sont les conditions pour créer une source authentique et comment contrôler la source authentique ?

1. *Raison opérationnelle* : avant de créer une source authentique, vous devez examiner dans quelle mesure vos données sont demandées.

> 1. *Demandez à vos parties prenantes (autres services publics) de définir clairement les données dont elles ont besoin, et à quelle fréquence.*
>
> 2. *Évaluez si la demande des parties prenantes est assez étendue pour entreprendre des démarches ultérieures afin de rendre les données et la source authentiques.*

2. *Critères légaux :* un service public peut créer une source authentique si les données pour lesquelles il veut créer une source authentique répondent à l'ensemble des 3 critères suivants :

    1. L'enregistrement de la donnée et sa communication à divers destinataires découlent de missions attribuées par ou en vertu d'une loi, d'un décret ou d'une ordonnance.
    2. La donnée est correcte, complète, sécurisée et disponible.
    3. L'instance chargée de la collecte et de la gestion des données fournit des garanties relatives à l'exactitude, l'exhaustivité, la sécurité et la disponibilité de la donnée.

    Si les conditions ne sont pas toutes respectées (par exemple exactitude et exhaustivité non garanties), la source ne peut pas être reconnue comme authentique.

> 3. Contactez votre service juridique et demandez-lui son avis sur les missions légales qui s'appliquent à votre organisation et sur la façon dont la collecte des données que vous voulez intégrer à votre source authentique s'inscrit dans le cadre de ces missions. (*S'il n'existe pas de cadre légal pour l'enregistrement et le traitement de données dans la source authentique, il faut d'abord le créer).*
>
> 4. Évaluez vous-même les données que vous voulez enregistrer dans la source authentique :
>
> - Comment avons-nous collecté ces données ?
> - Avons-nous encore récemment validé ces données ?
> - Comment nous sommes-nous assurés que ces données étaient correctes ?
> - Comment nous sommes-nous assurés que ces données étaient complètes ?
> - Avons-nous un processus validé pour assurer la maintenance et la mise à jour de ces données ?
> - Comment assurons-nous la sécurité des données (p.ex. limitation de l'accès) ?

3. *Droit de propriété :* puisqu'une donnée authentique ne peut être enregistrée qu'une seule fois, il est important de vérifier que vous êtes le « propriétaire » des données et qu'un autre propriétaire n'a pas déjà été désigné.

5. Vérifiez sur la liste des sources authentiques publiée par la DG TD du SPF BOSA (*https://dt.bosa.be/fr/echange_de_donnees/sources_authentiques/apercu_sources_authentiques*) s'il existe déjà une autre source qui contient les mêmes données. Si cette source existe déjà, vous ne pouvez pas en être le propriétaire.

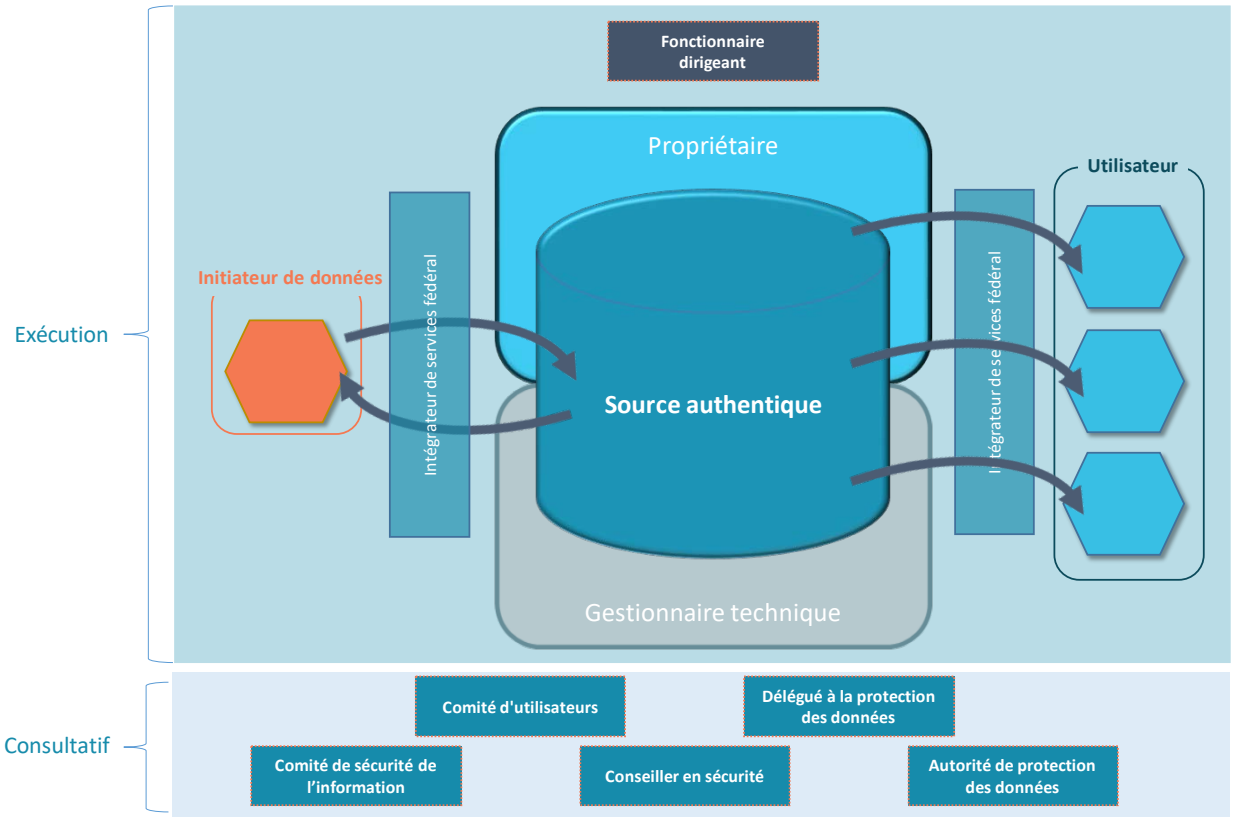
6. Si aucune source ne figure sur la liste de la DG TD de BOSA, vous devez vous assurer que d'autres services publics n'enregistrent pas de données similaires.

   À cette fin, vous pouvez contacter la DG TD du SPF BOSA (https://dtservices.bosa.be/fr/Contact/formulaire_de_contact) pour lui demander si elle connaît encore d'autres sources (non authentiques) contenant les mêmes données.
   Vous pouvez aussi contacter vous-même directement d'autres services publics pour leur demander s'ils enregistrent des données similaires et veulent les mettre à disposition sous forme de source authentique.

   Si on vous informe du fait qu'il existe d'autres sources contenant les mêmes données, vous devez contacter les propriétaires de ces sources afin de vous accorder sur qui est le « propriétaire » des données.

Lorsque le propriétaire d'une donnée ou d'une série de données a été déterminé, cette instance peut démarrer le processus en vue de la reconnaissance de la source authentique. Pour plus de détails sur le processus de la reconnaissance d'une source authentique, nous vous renvoyons à la Section 3 : « Comment rendre une source authentique disponible ? »

2.2 Quels sont les rôles et les responsabilités pour ma source authentique ?



Pour chaque source authentique, il existe différents rôles, tant pour la gouvernance (la direction de la source authentique) que pour l'exécution.

Dans le cadre de l'*exécution*, il convient de toujours définir au minimum 4 rôles :

- Initiateur de données
- Propriétaire
- Gestionnaire technique
- Utilisateur

Par ailleurs, une structure de *gouvernance* est établie pour chaque source.

D'une part, un *comité d'utilisateurs* est mis en place pour chaque source authentique. Ce comité est unique pour chaque source authentique et se compose des principaux intervenants (représentants des principaux utilisateurs, le propriétaire, le gestionnaire technique et les initiateurs de données).

Par ailleurs, deux rôles sont prévus pour la sécurité et la vie privée : le *conseiller en sécurité* et, si la source authentique contient des données à caractère personnel, il convient aussi de désigner un *délégué à la protection des données*. Le conseiller en sécurité et le délégué à la protection des données peuvent à leur tour faire appel aux 2 organismes suivants lorsqu'il s'agit de données à caractère personnel :

- Comité de sécurité de l'information
- Autorité de protection des données

Il s'agit d'instances officielles qui peuvent fournir des conseils au DPD sur la vie privée et la sécurité des données à caractère personnel.

Vous trouverez ci-dessous un aperçu résumé des activités typiques par rôle. Les responsabilités exactes peuvent différer d'une source authentique à l'autre, et doivent être fixées entre les parties dans un Service Level Agreement (voir section 2.5 : « Quels accords peuvent-ils être conclus entre les différentes parties ? »).

2.2.1 Exécution

L'Autorité de protection des données a identifié 4 phases de traitements de données à caractère personnel *(Recommandation n° 09/2012 du 23 mai 2012, Art. 6)* :

- Collecte : collecter des données et les documenter dans le format correct
- Validation : garantir que les données sont correctes
- Gestion : gestion de l'utilisation, application, maintenance, stockage de données
- Échange de données à caractère personnel.

Ci-dessous un aperçu des rôles impliqués dans ces phases.

	Collecte	Validation	Gestion	Échange
Initiateur de données	X	X		X
Propriétaire	X	X	X	X
Gestionnaire technique			X	X
Utilisateur				

Rôle : Initiateur de données

Description :

L'initiateur/les initiateurs de données est/sont la/les personne(s) responsable(s) du traitement ainsi que de l'*introduction et de la validation* des *données originales (authentiques).* L'initiateur de données est le premier interlocuteur pour les citoyens et entreprises.

Responsabilités :

- Acquérir des données par le biais des citoyens et entreprises
- Ajouter des données manquantes dans le système au moyen de documents officiels et/ou de la lecture électronique de données
- Enregistrer correctement de nouvelles données
- Modifier les données
- Vérifier l'exactitude et l'exhaustivité
- Échange des ensembles de données corrects avec le propriétaire via une procédure prédéfinie spécifiée via un SLA avec le propriétaire (voir Section 2.5 : « Quels accords peuvent-ils être conclus entre les différentes parties ? »)
- L'enregistrement d'un *audit log* selon les dispositions du SLA

Rôle : Propriétaire

Description :

Le propriétaire assume la *responsabilité finale* des données. Cela signifie que le propriétaire assume aussi la responsabilité finale de l'exactitude, l'exhaustivité, la disponibilité et la sécurité des données, ainsi que du *traitement* et de l'*échange* des données avec d'autres instances. Le propriétaire d'une donnée authentique est l'institution publique qui répond aux conditions suivantes :

- Le service public a une mission légale pour collecter et traiter les données.
- Le service public a, plus que d'autres services publics, un accès commun aux données et a déjà collecté la plupart des données.

Responsabilités :

- Traitement des données par le biais des initiateurs de données via une procédure prédéfinie spécifiée via un SLA avec l'initiateur de données (voir Section 2.5 : « Quels accords peuvent-ils être conclus entre les différentes parties ? »)
- Établir une stratégie pour la mise à jour de données avec l'initiateur de données
- Responsabilité finale de l'exactitude, l'exhaustivité, la disponibilité et la sécurisation de la source
- Échange des ensembles de données corrects avec d'autres instances via une procédure prédéfinie (voir section 3 : « Comment rendre une source authentique disponible ? »)
- L'enregistrement d'un *audit log* selon les dispositions du SLA.

Rôle : Gestionnaire technique

Description :

Le gestionnaire technique des données (authentiques) est l'instance qui est responsable de la *politique technique* relative à la captation, à l'enregistrement et à la maintenance des données ainsi qu'à leur ouverture destinée à l'intégrateur de services qui lui est propre. La connexion avec d'autres intégrateurs ou instances est dirigée par l'intégrateur de services associé. La politique technique relève de la responsabilité du propriétaire de la source.

Responsabilités :

Le gestionnaire technique assume notamment les tâches suivantes :

1. Déterminer et mettre en place la structure technique de la source
2. Déterminer et mettre en place le *modèle de données*
3. *Déterminer* les *interfaces* vers la source authentique
4. *Transposition* vers la *structure* correcte des données (par exemple XSD ou XML)
5. *Enrichissement* correct des *données* avec d'autres données du propriétaire, si cet enrichissement est réalisé au moyen d'un système.

La connexion avec d'autres intégrateurs ou instances est dirigée par l'intégrateur de services associé.

Rôle : Utilisateur

Chaque personne physique ou morale, y compris les entreprises, les institutions, les associations et toutes les composantes des autorités elles-mêmes, qui ont l'autorisation de consulter les données authentiques et de les utiliser à leurs propres fins.

Une autorisation peut provenir de l'organisme compétent (comité de sécurité de l'information ou Ministre de l'Intérieur) ou être basée sur un protocole établi entre le propriétaire et l'utilisateur.

Exemples :

Source	Initiateur(s) de données	Propriétaire	Gestionnaire technique

Registre national	• Communes	• SPF INT	• SPF INT
Banque Carrefour des Entreprises	• Tribunal de l'entreprise • Guichet d'entreprise • ONSS	• SPF Économie	• SPF Économie
Codes pays	• DG Statistique	• SPF Affaires étrangères	• SPF Économie

2.2.2 Gouvernance

Rôle : Comité d'utilisateurs

Description :

Le comité d'utilisateurs agit en tant qu'organisme commun responsable du *bon fonctionnement* du processus de collecte et d'échange de données. Il veille à ce que tous les *intervenants importants participent* au fonctionnement et à la politique de la source authentique. Ceci est conforme à l'avis de l'Autorité de protection des données (Recommandation n°09/2012 du 23 mai 2012). Pour chaque source authentique, il convient de créer un comité d'utilisateurs.

Responsabilités :

1. Harmonisation relative aux obligations communes, telles que reprises dans les Service Level Agreements conclus entre les parties concernées
2. Harmonisation relative à l'utilisation des différents systèmes utilisés pour la collecte, la validation, la gestion et l'échange des données avec les parties concernées
3. Fournir des avis pour l'optimisation du processus de collecte et d'échange de données
4. Harmonisation relative à la collaboration entre les parties prenantes ou le fonctionnement des systèmes utilisés

Rôle : Délégué à la protection des données (DPD)

Description :

Un délégué à la protection des données est désigné comme *expert* dans le domaine du traitement des données en vue de la *protection* et de la *sécurité* des *données à caractère personnel.*

Une instance publique est obligée de désigner un DPD conformément à l'article 37, 1, a) du Règlement européen 2016/679.

Un organisme privé qui traite des données à caractère personnel pour le compte d'une autorité publique fédérale ou à qui une autorité publique fédérale a transféré des données à caractère personnel désigne un délégué à la protection des données lorsque le traitement de ces données peut engendrer un risque élevé.

Responsabilités :

Conformément au RGPD, le DPD est responsable de ce qui suit :

1. *Informer* et *conseiller* les responsables de la gestion et du traitement des données (initiateurs de données, propriétaires et gestionnaires techniques)
   a. Les données ne peuvent être utilisées que dans le but pour lequel elles sont collectées.
   b. Ne pas enregistrer plus de données que le nombre nécessaire à la finalité de leur enregistrement.
   c. Les données ne peuvent pas être conservées plus longtemps que nécessaire.
2. *Vérifier* le respect des mesures de protection des données imposées par la législation belge et européenne en matière de protection des données.
3. *Premier point de contact* pour la sécurité et la protection des données à caractère personnel.
4. Gestion des formalités inhérentes au traitement de données, comme la rédaction d'un *protocole d'accord*. Les conseillers en sécurité des deux parties établissent une convention relative à l'échange de données. En cas de conflit, le comité de sécurité de l'information peut être consulté.

Rôle : Conseiller en sécurité

Description :

Un conseiller en sécurité offre des conseils et un accompagnement pour tous les aspects relatifs à la sécurité de l'information. Un conseiller en sécurité est désigné comme *expert* dans le domaine du traitement de données en vue de la *sécurité* des *données.*

Responsabilités :

1. *Informer* et *conseiller* les responsables de la gestion et du traitement des données
2. En *concertation* avec le *gestionnaire technique*, veiller à ce que le *traitement, la validation, la gestion et l'échange* des données se fasse de manière *sécurisée*.

Autorité de protection des données

Description :

L'Autorité de protection des données est l'institution publique belge qui veille à la *protection de la vie privée* dans le cadre du traitement de données à caractère personnel. L'Autorité de protection des données est, depuis l'entrée en vigueur du RGPD en mai 2018, le successeur de la Commission de la protection de la vie privée (CPVP), mieux connue sous l'appellation « Commission Vie privée » (Loi portant création de l'Autorité de protection des données, 3 décembre 2017).

Responsabilités :

- Fournir des conseils relatifs à la vie privée et à la sécurité dans le cadre du traitement de données à caractère personnel

Comité de sécurité de l'information (CSI)

Description :

Le comité de sécurité de l'information est un organisme indépendant qui détermine quelles *données à caractère personnel peuvent être échangées* et dans quelles *conditions de sécurité*.

Le CSI est constitué d'une chambre sécurité sociale et santé et d'une chambre autorité fédérale.

(Loi du 5 septembre 2018 instituant le comité de sécurité de l'information et modifiant diverses lois concernant la mise en œuvre du 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)

Attention ! L'accès aux données du Registre national ou aux données visées à l'art. 5, §2, de la loi relative au Registre national, ainsi que l'utilisation du numéro de Registre national, doivent être demandés au SPF Intérieur (article 5 de la loi du 08/08/1983 organisant un Registre national des personnes physiques).

Responsabilités :

- Octroyer une autorisation pour l'échange de données à caractère personnel entre la source authentique et les utilisateurs.

7. Octroyez les rôles exécutifs de la source authentique à des (parties d') organisations spécifiques :
   - Initiateur(s) de données
   - Propriétaire
   - Gestionnaire technique
   - Utilisateur(s)
8. Déterminez qui assumera le rôle de conseiller en sécurité et de DPD (si nécessaire)
9. Composez le comité d'utilisateurs et déterminez son mode de fonctionnement (fréquence, ordre du jour...)
10. Veillez à ce que les accords sur les responsabilités de chaque partie soient clairs et fixés dans des SLA et conventions d'utilisation (voir section 2.5). « Quels accords peuvent-ils être conclus entre les différentes parties ? »)

2.3 Comment choisir un modèle de données pour ma source authentique ?

Les instances publiques ne peuvent demander qu'une seule fois des données aux citoyens et aux entreprises *(Loi Only Once, 5 mai 2014).* Ces données sont ensuite *partagées à des fins de réutilisation* entre les différents services publics.

Une source authentique comprend uniquement des *données brutes*, sans aucune forme de logique d'entreprise. L'interprétation des données et l'ajout d'une logique d'entreprise spécifique se font en dehors de la source par le propriétaire ou les intégrateurs de services. Le propriétaire de la source peut éventuellement offrir des services supplémentaires avec la logique d'entreprise en plus des données génériques.

Il est dès lors important que le « modèle de données » de la source authentique soit bien décrit, et qu'il soit aussi publié afin que les autres instances publiques puissent en tenir compte.

Le modèle de données décrit *la façon dont les données sont enregistrées dans une source de données*, ainsi que le mode d'interaction entre ces données. Le modèle de données est généralement établi par un analyste fonctionnel ou un architecte IT avant le développement de la source de données.

Dans la description du modèle de données, il est recommandé d'évaluer les éléments suivants :

1. Période de validité
2. Contenu des données
3. Nomenclature : emploi des langues, noms, abréviations...
4. Exigences techniques
5. Unicité

Par ailleurs, de nombreux autres éléments peuvent être repris, en fonction des données et des besoins de votre source.

11. Rassemblez les attentes de vos parties prenantes : de quelles informations sur vos données *ont-elles besoin ?*

12. Demandez à votre architecte IT ou analyste de la source de données d'établir la description du modèle de données en fonction des questions que vous avez reçues de vos parties prenantes. Basez-vous sur les cadres d'interopérabilité (comme le « European Interoperability Framework ») afin de permettre une compatibilité et un échange maximaux.

2.4 Pourquoi et comment réaliser un *privacy audit log* et un *audit trail* ?

2.4.1 « Privacy audit log »

Une source authentique contient des données uniques, partagées avec l'ensemble des autorités et utilisées dans des processus et communications officiels des autorités. Il est dès lors important que l'on puisse en permanence contrôler quand et comment les données sont utilisées et modifiées, et que ces informations soient *opposables*.

C'est pourquoi la finalité et la proportionnalité des données dans une source authentique doivent être garanties :

- La *finalité* est un but bien déterminé, expressément défini et autorisé.
- La *proportionnalité* signifie que les données sont adéquates et pertinentes et ne peuvent pas être excessives au regard de la finalité pour laquelle elles sont obtenues et pour laquelle elles seront traitées ultérieurement. Les données ne peuvent pas non plus être conservées plus longtemps que la période strictement nécessaire à la finalité autorisée.

Afin de vérifier que chaque source authentique *respecte la législation applicable*, toutes les parties concernées doivent mettre en place un « privacy audit log ».

Un *« privacy audit log »* est un journal qui est automatiquement généré par le système et qui comprend des informations sur la *consultation* ou la *création, l'adaptation et la suppression* de *données*. Ce journal est créé par chaque système impliqué dans la mise en place et l'exécution de la source authentique. Ces informations vous permettent de vérifier en tout temps pour chaque système quelles données ont été consultées ou manipulées. Le journal capte généralement les informations suivantes sur la consultation ou la modification :

1. L'ID unique des utilisateurs (qui)
2. La date et l'heure (quand)
3. Le type de consultation/modification
4. L'ancienne et la nouvelle valeur de la donnée (quoi)

Outre ces informations, les parties concernées doivent déterminer quelles autres informations doivent encore être reprises dans le « privacy audit log ».

Un « privacy audit log » doit généralement rester disponible pendant 10 ans. Vu que les données du « privacy audit log » peuvent aussi être à caractère personnel, elles doivent ensuite être supprimées. Pour chaque source authentique, il faut cependant déterminer individuellement combien de temps les données doivent rester disponibles, en fonction des exigences légales.

2.4.2 « Privacy audit trail »

En rassemblant les « audit logs » de tous les systèmes des parties de la chaîne (organisation utilisatrice, intégrateur de services, gestionnaire de la source), un « privacy audit trail » peut être reconstitué afin de refléter quel utilisateur final a procédé à une demande spécifique, à quel moment et dans quel contexte.

Cet *audit trail* permet de reconstituer les transactions effectuées via l'intégrateur de services afin de respecter l'obligation légale relative aux données à caractère personnel. Chaque partenaire de la chaîne (initiateur de données, propriétaire et utilisateur) reste cependant responsable des « audit logs » sur ses propres systèmes.

13. Discutez avec l'initiateur de données, le propriétaire et l'utilisateur de la source authentique de la façon de mettre en place les « audit logs », des informations à y intégrer et de la façon de créer un « audit trail ». Dans ce cadre, veuillez tenir compte des points suivants :

- **Sécurité** : veillez à ce que chaque « privacy audit log » soit sécurisé et ne puisse être adapté, supprimé ou désactivé. Seul un utilisateur privilégié (p.ex. administrateur) du système peut adapter, supprimer ou désactiver les données de l'« audit log » en suivant une procédure contrôlée. Ces actions sont également tenues à jour par le système.

- **Disponibilité** : l'audit trail doit être reconstitué jusqu'à 10 ans (sauf exigences légales contraires). En cas d'enquête, les données doivent pouvoir être fournies dans les 24h sur demande. Les données que contient le « privacy audit log » doivent pouvoir être imprimées ou exportées. Les données de l'audit trail doivent être supprimées à l'échéance du délai de conservation légal.

- **Vie privée** : Idéalement, on offre *aussi* au citoyen *la possibilité de rechercher* qui a consulté *ses* données, et à quelles fins, au cours des mois écoulés (p.ex. via une application web comme « Mon Dossier » pour le Registre national). Le propriétaire de la source authentique peut

choisir lui-même la procédure et l'infrastructure qui lui permettront de répondre à ces exigences de manière sécurisée et dans le respect de la vie privée.

Pour plus d'informations légales et techniques sur la mise en place d'un « privacy audit trail », vous pouvez toujours consulter le manuel « La mise en place d'une piste d'audit : manuel à l'attention des partenaires de la chaîne de Fedict »

2.5 Quels accords peuvent-ils être conclus entre les différentes parties ?

Afin de satisfaire les utilisateurs, il est important de prédéfinir leur attentes correctement au préalable, et de les clarifier autant que possible dans des accords formels. Ces derniers peuvent être repris dans des conventions d'utilisation ou « Service Level Agreements » (SLA).

La convention d'utilisation définit *les droits et obligations* liés à l'utilisation de la source authentique. Elle comprend généralement :

- une description du service ;
- les conditions d'utilisation du service (coûts, finalités, volumes, etc.) ;
- les accords relatifs à la sécurité (p.ex. autorisations, « audit trail »...).

La « convention d'utilisation FSB » peut servir d'exemple (voir https://dtservices.bosa.be/fr/services/fsb/demande-dun-service-web-fsb-ou-dun-certificat-fsb/je-demande-dacceder-un-service-web)

Un *Service Level Agreement (SLA)* est une *convention* visant à coordonner l'*échange d'informations* entre les 2 parties concernées. Il peut être repris dans la convention d'utilisation ou être conclu distinctement. Un SLA comprend une série de conditions et composantes à respecter par les deux parties. Un SLA peut être rédigé entre le propriétaire et l'utilisateur ou entre le propriétaire et la partie responsable de l'ouverture de la source (intégrateur de services).

Le SLA comprendra idéalement les parties suivantes :

1. **Nature des données :**
   - Nom des données
   - Brève description des données
   - Objectif de la conservation de ces données
2. **Procédures :**
   - Procédures qui assurent que les caractéristiques typiques (exactitude, exhaustivité, sécurité et disponibilité) d'une source authentique sont garanties en cas de collecte, validation et échange des données authentiques
   - Procédures qui assurent la validation et l'adaptation d'une correction ou mise à jour d'une donnée, par le biais d'un processus défini au préalable
3. **Rôles et responsabilités :**
   - Le rôle de l'initiateur de données
   - Le rôle du propriétaire
   - Le rôle du gestionnaire technique
   - Le rôle du comité d'utilisateurs
   - (voir Section 2.2 : Quels sont les rôles et les responsabilités pour ma source authentique ?)
4. **« Privacy audit log » :**
   - Définition du responsable de l'enregistrement du « privacy audit log » pour chaque partie concernée et du responsable de la reconstitution de « l'audit trail » en cas de demande (voir Section 2.4 : Pourquoi et comment réaliser un *privacy audit log* et un *audit trail* ?)
5. **Exigences techniques :**
   - Gestion des changements et des versions
     - Déterminer le processus relatif à la proposition de modifications

    - Maintenance des systèmes (p.ex. moments prédéfinis pour des mises à jour ou mises à niveau)
- Disponibilité des systèmes (p.ex. 24H/24, 7j/7 ou pendant les heures de bureau)
- Possibilités de connexions aux systèmes (p.ex. basées sur le web)
- Performance des systèmes (p.ex. temps de réponse en x millisecondes)
- Restrictions de capacité des systèmes (p.ex. nombre d'utilisateurs actifs par minute)
- Le suivi de notifications d'incidents sur les systèmes et le temps de réaction prévu (p.ex. les incidents de priorité élevée doivent être résolus dans un délai de 4 heures).

Les parties ci-dessus sont cependant des directives. On peut consulter le comité d'utilisateurs pour des avis sur d'autres aspects importants qui doivent être repris dans cette convention.

14. Demandez au comité d'utilisateurs quels éléments (processus, responsabilités…) doivent être définis, et veillez à ce qu'ils soient repris de manière claire et exhaustive.

3 Comment rendre une source authentique disponible ?

Cette section permet de mieux comprendre comment une source authentique peut être ouverte. À cette fin, 2 étapes sont nécessaires, à savoir :

1. Reconnaître la source comme authentique : les sections précédentes expliquent déjà ce qu'est une source authentique et comment la mettre en place. La présente section examine en détail comment une source authentique peut aussi être reconnue.
2. Enfin, une source doit être ouverte, afin que les données puissent être demandées par les utilisateurs autorisés à cette fin.

3.1 Comment ajouter ma source à la liste publiée de sources authentiques de l'intégrateur de services fédéral ?

Le processus de publication d'une source authentique peut se faire de deux manières.

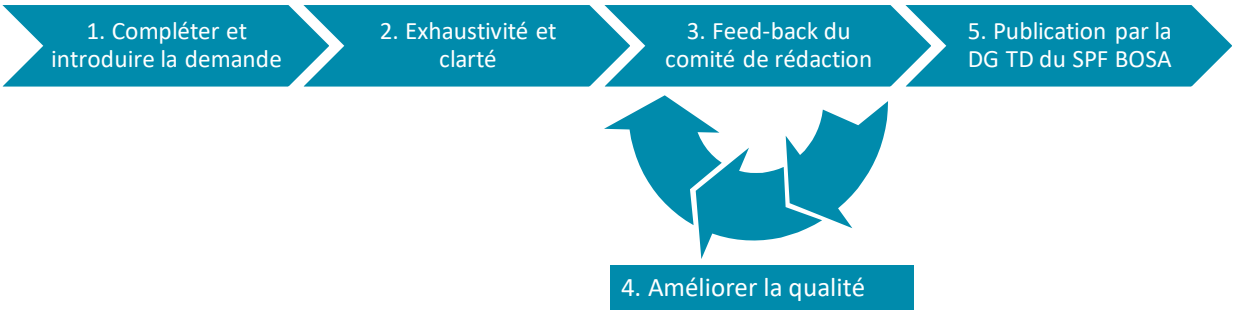
3.1.1 Publication en tant que source authentique via un Arrêté royal

Une source de données peut être déclarée source authentique si un Arrêté royal ou une loi a été approuvé(e) à cette fin. Après publication au Moniteur belge, les données de votre source authentique peuvent être reprises par le SPF BOSA dans la liste des sources authentiques.

3.1.2 Publication en tant que source authentique par le comité de rédaction

Remarque : cette procédure n'est pas encore finalisée. Toutes les informations de cette section sont sujettes à des modifications. En cas de modification, la DG TD du SPF BOSA publiera une nouvelle version de ce document.

Le comité de coordination de l'intégrateur de services fédéral, dans lequel toutes les autorités participantes sont représentées, a désigné un « Comité de rédaction Sources authentiques ». Ce dernier est mandaté pour évaluer que des sources de données potentielles satisfont aux exigences d'une source authentique, et pour les intégrer à la liste des sources authentiques.



1. Si l'on souhaite que ce soit l'intégrateur de services fédéral qui publie la source authentique, il convient de compléter le modèle de document relatif à la publication (voir Section 4 : « Formulaire de demande de publication »). La demande est introduite à la DG TD du SPF BOSA via *https://dtservices.bosa.be/fr/Contact/formulaire_de_contact*
2. L'intégrateur de services fédéral se concerte avec le demandeur afin de garantir l'exhaustivité et la clarté de la demande.

3. L'intégrateur de services fédéral transmet la demande aux membres du comité de rédaction. Les membres du comité de rédaction ont 3 semaines (à confirmer) pour donner leur feed-back. En l'absence de feed-back, la demande est approuvée.
4. L'intégrateur de services fédéral soutient le demandeur afin d'accroître la qualité de la source authentique.
5. En cas d'acceptation de la demande, le propriétaire est informé et l'intégrateur de services fédéral ajoute la source à la liste des sources authentiques et prévoit des liens vers les informations du propriétaire sur la source authentique, qui doit la publier :

    1. Les *caractéristiques* de la donnée telles que le contenu, le mode d'enregistrement, la périodicité des adaptations et les spécifications techniques
    2. Les procédures pour l'*enregistrement*
    3. La *gestion* de la donnée et la *répartition des tâches* pendant chaque phase de l'enregistrement
    4. La procédure pour l'*accessibilité* de la donnée
    5. La procédure pour continuer à assurer l'*exactitude*, l'*exhaustivité*, la *sécurité* et la *disponibilité* de la donnée
    6. *Accords transparents* avec le service public qui souhaite utiliser la donnée
    7. La procédure pour *signaler* des erreurs dans la donnée et pour *corriger* la donnée
    8. Concertation en vue de l'amélioration de la *qualité*, de la *disponibilité* et de l'*utilisation* de la donnée
    9. La description des façons dont la *personne concernée* peut *exercer ses droits* à l'égard des données à caractère personnel traitées à son sujet.

3.2 Comment ouvrir ma source ?

Le propriétaire et le gestionnaire technique de la source authentique déterminent la façon dont ils veulent ouvrir la source authentique. Ce choix dépend du type de données offertes et de la façon dont l'utilisateur utilise ces données.

Par le biais de l'intégrateur de services fédéral, l'ouverture peut se faire efficacement et on garantit que l'accès aux sources authentiques et l'échange rapide des données se font de manière sécurisée et homogène.

Voici quelques possibilités d'ouverture d'une source authentique :

1. Service web : via la technologie de REST ou SOAP
2. File Transfer Protocol (FTP)
3. HTML
4. Excel
5. Publication site web
6. …

Par ailleurs, ils doivent faire un choix de fréquence (temps réel ou traitement en lots) du traitement des données et de la disponibilité de la source (continue ou périodique). Pour ces décisions, le propriétaire peut tenir compte des avis du comité de coordination, du conseiller en sécurité et du gestionnaire technique. Le gestionnaire technique doit ensuite offrir le soutien technologique nécessaire pour les décisions relatives à l'ouverture de la source authentique.

Généralement, l'ouverture de la source authentique comprend les activités suivantes :

- Établissement de la description fonctionnelle de la source
- Définir des cas de test
- Mettre en place un environnement de test, éventuellement avec des données anonymisées
- Documentation des codes d'erreurs fonctionnels et techniques.

Pour plus d'informations sur ces activités, vous pouvez contacter la DG TD du SPF BOSA.

4 Formulaire de demande de publication

Ce formulaire de demande vous permet de compléter toutes les données de votre source authentique éventuelle. Vous devez aussi utiliser cette liste de vérification quand vous introduisez votre demande de publication (voir section 3.1.2 : « Publication en tant que source authentique par le comité de rédaction »).

1. « Business case »

Décrivez brièvement l'objectif de votre source authentique et les utilisateurs éventuels qui peuvent demander ces données.

2. Mission légale

Veuillez indiquer quelle base légale, ordonnance ou autre information s'applique à votre organisation, de laquelle vous concluez que vous avez la mission légale de collecter et enregistrer ces données dans une source authentique :

3. Description de la source authentique :

Décrivez quelles données vous allez enregistrer dans la source authentique

4. Garantie de l'exactitude et de l'exhaustivité :

Décrivez comment vous garantissez que vos données sont complètes et correctes et comment vous garantissez qu'elles resteront complètes et correctes à l'avenir également.

Existe-t-il une procédure de feed-back (p.ex. point de contact) pour corriger des erreurs ?

5. Rôles

Indiquez qui assumera les rôles suivants :

Initiateur(s) de données	*Qui introduira et adaptera les données si nécessaire ?*
Propriétaire	*Qui sera le propriétaire de votre source authentique ?*
Gestionnaire technique	*Qui assumera la politique technique de votre source authentique ?*
Utilisateur(s)	*Qui sont les utilisateurs potentiels de votre source authentique ?*
Comité d'utilisateurs	*Comment le comité d'utilisateurs sera-t-il composé ?*
Délégué à la protection des données	*Quelle personne fera office de DPD pour votre source authentique ?*
Conseiller en sécurité	*Quelle personne fera office de conseiller en sécurité pour votre source authentique ?*

6. *Privacy audit log & trail*

Veuillez indiquer que vous satisfaites aux aspects suivants des « privacy audit logs » :

Chaque système impliqué dans ma source authentique a un « privacy audit log »	*Oui/Non*
Les « privacy audit logs » de tous les systèmes sont tenus à jour pendant 10 ans	*Oui/Non*
Les données des « privacy audit logs » peuvent être fournis dans les 24h sur demande	*Oui/Non*

7. Modèle de données

Listez brièvement les attentes de vos parties prenantes : de quelles informations sur vos données ont-elles besoin ?

Traduisez la liste ci-dessus en éléments de données concrets et uniques.

8. *Service Level Agreement* (Contrat de niveau de service)

Un Service Level Agreement est-il prévu entre toutes les parties concernées ? Si non, motivez brièvement pourquoi.

Le comité d'utilisateurs a-t-il été consulté pour un avis sur ce qu'il faut reprendre dans le(s) Service Level Agreement(s) ?

Que faut-il décrire dans le(s) Service Level Agreement(s) sur la nature des données ?

Quelles exigences techniques doivent être reprises dans le(s) Service Level Agreement(s) pour l'échange des données ?

5 Définitions

Source authentique	*« Une source authentique est une banque de données dans laquelle sont conservées des données authentiques » (Loi relative à la création et à l'organisation d'un intégrateur de services fédéral, 15 août 2012, Art. 2).* Ces données sont reconnues comme originales et constituent par conséquent la source la plus fiable. Les sources authentiques veillent à ce que les données sur une personne ou une entreprise ne soient collectées qu'une seule fois. *Vous trouverez des informations détaillées sur les sources et données authentiques au chapitre 1.*
Donnée authentique	*« Il s'agit d'une donnée qu'une instance collecte et gère dans une banque de données et qui a valeur de donnée unique et originale concernant une personne ou un fait juridique, de sorte que les autres instances ne peuvent ni ne doivent plus collecter cette même donnée » (Loi relative à la création et à l'organisation d'un intégrateur de services fédéral, 15 août 2012, Art. 2).* *Vous trouverez des informations détaillées sur les sources et données authentiques au chapitre 1.*
Comité de coordination (de l'intégrateur de services fédéral)	*« Le comité de coordination conseille l'intégrateur de services fédéral en ce qui concerne :* 1. *l'ouverture possible des banques de données ou sources authentiques par le biais de l'intégrateur de services fédéral ;* 2. *la possible adaptation des sources authentiques sélectionnées, de sorte que seules des données authentiques soient ouvertes dans la mesure du possible ;* 3. *l'utilisation de renvois à la donnée authentique dans la source authentique en ce qui concerne les données qui recouvrent, partiellement ou dans leur ensemble, une donnée authentique dans une source authentique ;* 4. *l'établissement d'une banque de règles pour une ou plusieurs banques de données ;* 5. *le partage de la responsabilité entre l'intégrateur de services fédéral, les services publics participants et les intégrateurs de services, compte tenu des compétences qui leur sont conférées par la présente loi. »* *(Loi relative à la création et à l'organisation d'un intégrateur de services fédéral, 15 août 2012, Art. 27, §1er).*

Modèle de données	Le modèle de données décrit la façon dont les données sont enregistrées dans la source de données, ainsi que le mode d'interaction entre ces données. Le modèle de données est généralement établi par un analyste fonctionnel ou un architecte IT avant le développement de la source de données. *Vous trouverez des informations détaillées sur le modèle de données au chapitre 2.3.*
Délégué à la protection des données (DPD)	Le RGPD du 25 mai 2018 oblige toutes les instances publiques à introduire un rôle de délégué à la protection des données. Le DPD est désigné comme expert dans le domaine du traitement des données afin de garantir leur confidentialité et leur sécurité conformément au RGPD du 25 mai 2018. *Vous trouverez des informations détaillées sur le DPD au chapitre 2.2.*
Intégrateur de services	*« Un intégrateur de services est une institution qui, par ou en vertu d'une loi, est chargée de l'intégration de services à un niveau de pouvoir ou dans un secteur déterminé »* (Loi relative à la création et à l'organisation d'un intégrateur de services fédéral, 15 août 2012, Art. 2). L'intégration de services est l'organisation d'échanges mutuels de données électroniques entre instances et l'ouverture intégrée de ces données. Il existe 3 intégrateurs de services fédéraux : - La DG Transformation digitale du SPF BOSA (anciennement Fedict) - e-Health - La Banque Carrefour de la Sécurité sociale
Propriétaire	Le propriétaire est l'un des rôles nécessaires à la gestion d'une source authentique. Le propriétaire assume la responsabilité finale des données. Cela signifie qu'il assume aussi la responsabilité finale de l'exactitude, l'exhaustivité et la disponibilité des données, ainsi que du traitement et de l'échange des données avec d'autres instances. *Vous trouverez au chapitre 2.2 des informations détaillées sur les rôles liés à la gestion d'une source authentique.*
Loi Fedict	« La loi du 15/08/2012 relative à la création et à l'organisation d'un intégrateur de services fédéral » est généralement connue sous la dénomination « Loi Fedict ».

	La DG TD du SPF BOSA (anciennement Fedict) a, dans ce cadre, été nommée intégrateur de services. Sa mission est de simplifier et d'optimiser l'échange de données entre d'une part les services publics participants (à savoir l'ensemble des services publics fédéraux et institutions publiques fédérales sauf ceux relevant de la Sécurité sociale) mutuellement, et d'autre part entre les services publics participants et les autres intégrateurs de services.
Utilisateur	Chaque personne physique ou morale, y compris les entreprises, les institutions, les associations et toutes les composantes des autorités elles-mêmes, qui ont l'autorisation de consulter les données authentiques et de les utiliser à leurs propres fins. Cette autorisation est octroyée sur la base de l'avis de l'autorité de protection des données.
Comité d'utilisateurs	Chaque source authentique doit disposer d'un comité d'utilisateurs. Le comité d'utilisateurs agit en tant qu'organisme commun responsable du bon fonctionnement du processus de collecte et d'échange de données. Il veille à ce que tous les intervenants importants participent au fonctionnement et à la politique de la source authentique. (Avis 18/2012 de la Commission de la protection de la vie privée, 23 mai 2012). *Vous trouverez des informations détaillées sur les rôles d'une source authentique à la Section 2 : « Comment mettre en place une source authentique ? ».*
Autorité de protection des données	L'Autorité de protection des données est l'institution publique belge qui veille à la protection de la vie privée dans le cadre du traitement de données à caractère personnel. L'Autorité de protection des données est, depuis l'entrée en vigueur du RGPD le 25 mai 2018, le successeur de la Commission de la protection de la vie privée (CPVP), mieux connue sous l'appellation « Commission Vie privée » (Loi portant création de l'Autorité de protection des données, 3 décembre 2017, Art. 2 & Art. 4).
Initiateur de données	L'initiateur de données est l'organisation responsable de la collecte, de la saisie, de la validation et de la correction de données. *Vous trouverez des informations détaillées sur les rôles d'une source authentique à la section 2.2.*

Règlement général sur la protection des données (RGPD)	Le RGPD est un Règlement européen (en vigueur depuis le 25 mai 2018) qui a été harmonisé avec la législation européenne relative à la vie privée. Le RGPD a pour objectif de mieux protéger les données à caractère personnel des individus. Cette loi a deux champs d'application. Elle s'applique d'une part au traitement de données à caractère personnel par des entreprises et organisations européennes, indépendamment de l'endroit où ce traitement s'effectue. D'autre part, la loi s'applique au traitement des données à caractère personnel de ressortissants de l'U.E. par des entreprises qui ne sont pas établies au sein de l'U.E., quand ces entreprises proposent des biens ou des services à ces ressortissants au sein de l'U.E., ou surveillent le comportement de ressortissants de l'U.E., dans la mesure où il s'agit de leur comportement au sein de l'Union. (Règlement général sur la protection des données, 25 mai 2018)
Comité de sécurité de l'information (CSI)	Le comité de sécurité de l'information est un organisme indépendant qui détermine quelles données à caractère personnel peuvent être échangées et dans quelles conditions de sécurité. Le CSI est constitué d'une chambre sécurité sociale et santé et d'une chambre autorité fédérale. (Loi du 5 septembre 2018 instituant le comité de sécurité de l'information et modifiant diverses lois concernant la mise en œuvre du 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)
Loi « Only Once »	*« La loi du 5 mai 2014 garantissant le principe de la collecte unique des données dans le fonctionnement des services et instances qui relèvent de ou exécutent certaines missions pour l'autorité et portant simplification et harmonisation des formulaires électroniques et papier »* est généralement connue sous le nom de la loi « Only Once ». Cette loi stipule que les instances doivent réutiliser les données déjà disponibles issues des sources (authentiques)au lieu de les redemander aux citoyens et entreprises. Il convient de souligner l'importance d'un échange de données correct entre les différentes instances.
« Privacy audit log »	Un « privacy audit log » comprend des informations relatives à la consultation ou à la modification de données – création, adaptation et suppression – qui sont générées automatiquement

	par le système. Ces informations vous permettent de vérifier en tout temps pour chaque système quelles données ont été consultées ou manipulées. *Vous trouverez des informations détaillées sur le « privacy audit log & trail » à la section 2.4*.
« Privacy audit trail »	Un « privacy audit trail » est constitué en rassemblant les « audit logs » des différents partenaires de la chaîne. Cet *audit trail* garantit que les transactions effectuées via l'intégrateur de services peuvent être reconstituées afin de respecter l'obligation légale (*Loi relative à la protection de la vie privée, 8 décembre 1992, Art. 16*). *Vous trouverez des informations détaillées sur le « privacy audit log & trail » à la section 2.4*.
« Service Level Agreement »	Un « Service Level Agreement » (SLA) est une convention visant à coordonner l'échange d'informations entre les 2 parties impliquées. Un SLA comprend une série de conditions et composantes à respecter par les deux parties. *Vous trouverez des informations détaillées sur les SLA à la section 2.5.*
Gestionnaire technique	Le gestionnaire technique des données (authentiques) est l'instance qui, sous la responsabilité du propriétaire, se charge de la politique technique relative à la captation, à l'enregistrement et à la maintenance des données ainsi qu'à leur ouverture destinée à l'intégrateur de services qui lui est propre. La connexion avec d'autres intégrateurs ou instances est dirigée par l'intégrateur de services associé. *Vous trouverez des informations détaillées sur les rôles d'une source authentique à la section 2.*
Conseiller en sécurité	Un conseiller en sécurité offre des conseils et un accompagnement pour tous les aspects relatifs à la sécurité de l'information. Un conseiller en sécurité est désigné comme expert dans le domaine du traitement des données en vue de la sécurité des données.