Erstellung einer authentischen Quelle

Fassung 1 – März 2019

FÖD BOSA DG Digitale Transformation

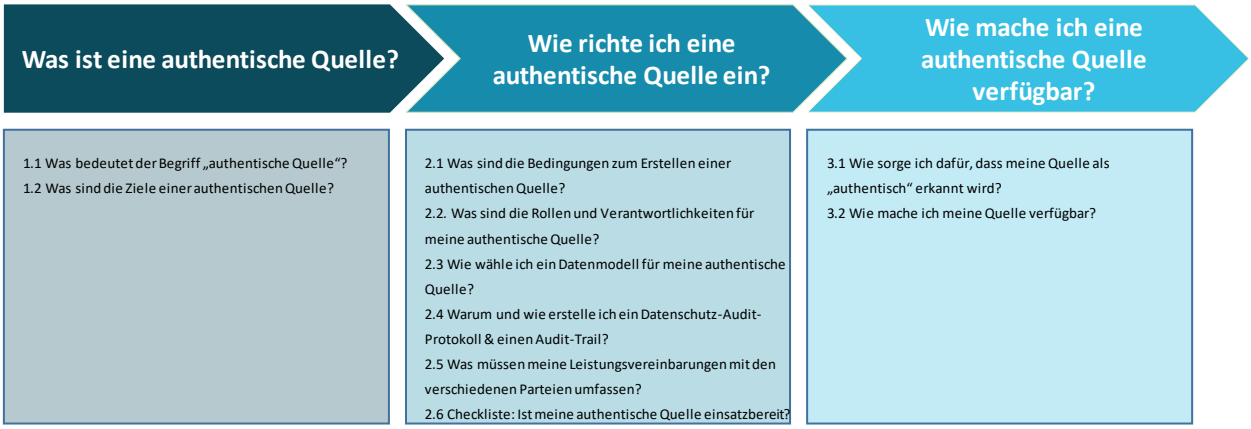
Federale overheidsdienst
Beleid en Ondersteuning
Service public fédéral
Stratégie et Appui

INHALT

Übersicht

In diesem Dokument werden die typischen Aktivitäten und Schwerpunkte zur Erstellung einer authentischen Quelle beschrieben. Die Informationen in diesem Dokument dienen dazu, andere öffentliche Dienste zu unterstützen und die Erstellung authentischer Quellen zu beschleunigen.

Jede authentische Quelle ist jedoch einzigartig hinsichtlich der Erwartungen, der Nutzung und des Zwecks. Der Inhaber der Quelle bleibt weiterhin dafür verantwortlich, die Aktionen korrekt durchzuführen und zusätzliche Aktionen festzulegen, um zu gewährleisten, dass die Quelle gut funktioniert, alle einschlägigen Gesetzes- und Rechtsvorschriften eingehalten werden und die Erwartungen der Interessengruppen erfüllt werden.



Die Begriffe und deren Erläuterung finden Sie in Abschnitt 5.

1 Was ist eine authentische Quelle?

1.1 Der Begriff „Authentische Quelle“

„Eine authentische Quelle ist eine Datenbank, in der authentische Daten gespeichert sind. Diese Daten gelten als einzige und ursprüngliche Daten bezüglich der betreffenden Person oder Rechtstatsache.“ (Gesetz über die Schaffung und Organisation eines föderalen Dienste-Integrators, 15. August 2012, Artikel 2).

Eine authentische Quelle gilt als die Referenz schlechthin, um bestimmte Daten zu erhalten und bietet spezifische Garantien hinsichtlich der *Richtigkeit*, der *Vollständigkeit* und *Verfügbarkeit* dieser Daten.

- Richtigkeit: Daten, die aus einer authentischen Quelle abgerufen werden, können als korrekt und aktuell betrachtet werden.
- Vollständigkeit: Die authentische Quelle enthält die vollständige Datenpopulation.
- Verfügbarkeit: Die authentische Quelle kann von den diesbezüglich ordnungsgemäß berechtigten Personen in vorher festgelegten Zeitintervallen abgerufen werden.

Zweck einer authentischen Quelle ist es, die administrativen Verpflichtungen der Bürger und der juristischen Personen zu *verringern*, indem sie ihnen garantiert, dass Daten, die für die Behörden bereits in einer authentischen Quelle verfügbar sind, einem föderalen öffentlichen Dienst nicht erneut mitgeteilt werden müssen.

Eine authentische Quelle erfüllt daher eine zentrale Rolle für mehrere Zwecke:

1. Die natürlichen und juristischen Personen müssen diese Daten im Grunde *nur einmal dieser Quelle übermitteln.*
2. Eine authentische Quelle wird für andere öffentliche Dienste zugänglich gemacht, damit sie diese Daten aus dieser Quelle abrufen können und sie *nicht länger einzeln* für die Erhebung der gleichen Informationen sorgen müssen.

(Only-once-Gesetz, 5. Mai 2014, Artikel 2).

1.2 Was sind die Vorteile einer authentischen Quelle?

Authentische Quellen bringen sowohl der Instanz, die als Quelleninhaber auftritt, als auch den Nutzern der authentischen Daten und den Bürgern/Unternehmen Vorteile.

1. Höhere Datenqualität

Durch die *Garantien und Verfahren* ist die Qualität der Daten in einer authentischen Quelle bereits hoch. Außerdem werden mehr Menschen dieselben Daten verwenden, wodurch etwaige Fehler schneller festgestellt und berichtigt werden, sodass die Qualität der Daten weiter zunimmt.

2. Weniger Duplikate

Die Daten müssen nicht mehr in lokalen Datenbanken bei verschiedenen Instanzen dupliziert werden. Dadurch können die öffentlichen Dienste jederzeit über die *aktuellsten Daten* verfügen.

3. Niedrigere Verwaltungskosten

Bei einer Änderung der Daten muss *nur einmal eine einzige Quelle* angepasst werden. Verwaltung, Schutz und Wartung der Daten müssen nur an einem einzigen Ort durchgeführt werden.

4. Garantierte Verfügbarkeit

Angesichts der Verfügbarkeitsgarantien haben alle Nutzer *einen klaren Einblick in die Zeiträume,* in denen sie auf die Daten zugreifen können.

5. Einmalige Eingabe

Bürger und Unternehmen müssen den Behörden *nur einmal ihre Daten übermitteln.* Danach sind die Behörden verpflichtet, diese Daten zugänglich zu machen und wiederzuverwenden.

6. Höhere Sicherheit

Durch die deutliche Bezeichnung der *Rollen,* die für die Sicherheit verantwortlich sind (DPO und Sicherheitsberater) und durch die Erstellung von *Verfahren* für die Verarbeitung, Speicherung und den Austausch der Daten kann die Sicherheit erhöht und ein nicht autorisierter Zugriff auf die Daten vermieden werden.

7. Zugänglichkeit

Wenn die Quelle als authentische Quelle anerkannt wird, wird sie zur *Liste auf der Website des FÖD BOSA* hinzugefügt. Alle Nutzer, die diese Daten für ihre eigenen Zwecke benötigen, können auf diese Weise *leicht* den Inhaber finden und, falls erforderlich, *eine Zugriffsberechtigung* bei der befugten Instanz beantragen.

2 Wie erstelle ich eine authentische Quelle?

2.1 Was sind die Bedingungen zur Erstellung einer authentischen Quelle und wie kann ich diese kontrollieren?

1. *Geschäftsgrund*: Bevor Sie eine authentische Quelle erstellen, müssen Sie überprüfen, in welchem Umfang Ihre Daten abgerufen werden.

1. Bitten Sie Ihre Interessengruppen (andere öffentliche Dienste), die von ihnen benötigten Daten deutlich anzugeben und wie oft sie diese benötigen werden.

2. Beurteilen Sie, ob die Anfrage der Interessengruppen groß genug ist, um weitere Schritte zur Authentisierung der Daten und der Quelle zu unternehmen.

2. *Rechtliche Kriterien:* Ein öffentlicher Dienst kann eine authentische Quelle erstellen, wenn die Daten, für die man eine authentische Quelle erzeugen möchte, alle folgenden 3 Kriterien erfüllen:

    1. Die Erfassung der Information und deren Mitteilung an verschiedene Empfänger ergibt sich aus Aufgaben, die durch oder aufgrund eines Gesetzes, eines Dekrets oder einer Ordonnanz anvertraut werden.
    2. Die Daten sind korrekt, vollständig, gesichert und verfügbar.
    3. Die Instanz, die für die Erhebung und Verwaltung der Daten verantwortlich ist, gibt Garantien hinsichtlich der Richtigkeit, Vollständigkeit, Sicherheit und Verfügbarkeit der Information.

    Falls nicht alle Bedingungen erfüllt sind (wenn beispielsweise die Richtigkeit und Vollständigkeit nicht garantiert sind), kann die Quelle nicht als authentisch anerkannt werden.

3. Nehmen Sie Kontakt mit Ihrer Rechtsabteilung auf und bitten Sie sie um Rat bezüglich der gesetzlich vorgeschriebenen Aufträge, die auf Ihre Organisation anwendbar sind, und wie die Erhebung der Daten, die Sie in der authentischen Quelle speichern möchten, in diesem Rahmen erfolgt. (*Falls es keinen Rechtsrahmen für die Speicherung und Verarbeitung von Daten in der authentischen Quelle gibt, muss dieser zuerst geschaffen werden.)*

4. Führen Sie eine Selbstevaluation bezüglich der Daten durch, die Sie in der authentischen Quelle speichern möchten:

- Wie haben wir diese Daten erhoben?
- Haben wir die Daten noch vor Kurzem validiert?
- Wie haben wir sichergestellt, dass die Daten richtig sind?
- Wie haben wir sichergestellt, dass die Daten vollständig sind?
- Haben wir ein validiertes Verfahren, um die Daten zu pflegen und auf dem neuesten Stand zu halten?
- Wie gewährleisten wir die Sicherheit der Daten (beispielsweise dass der Datenzugriff beschränkt ist)?

3. *Inhaberschaft:* Weil authentische Daten nur einmal gespeichert werden können, ist es wichtig, zu überprüfen, dass Sie „der Inhaber“ der Daten sind und nicht bereits ein Inhaber zugewiesen wurde.

5. Sehen Sie in der vom FÖD BOSA DT (weblink) veröffentlichten Liste der authentischen Quellen nach, ob es nicht schon andere Quellen mit denselben Daten gibt. Wenn diese Quelle bereits existiert, können Sie kein Inhaber sein.

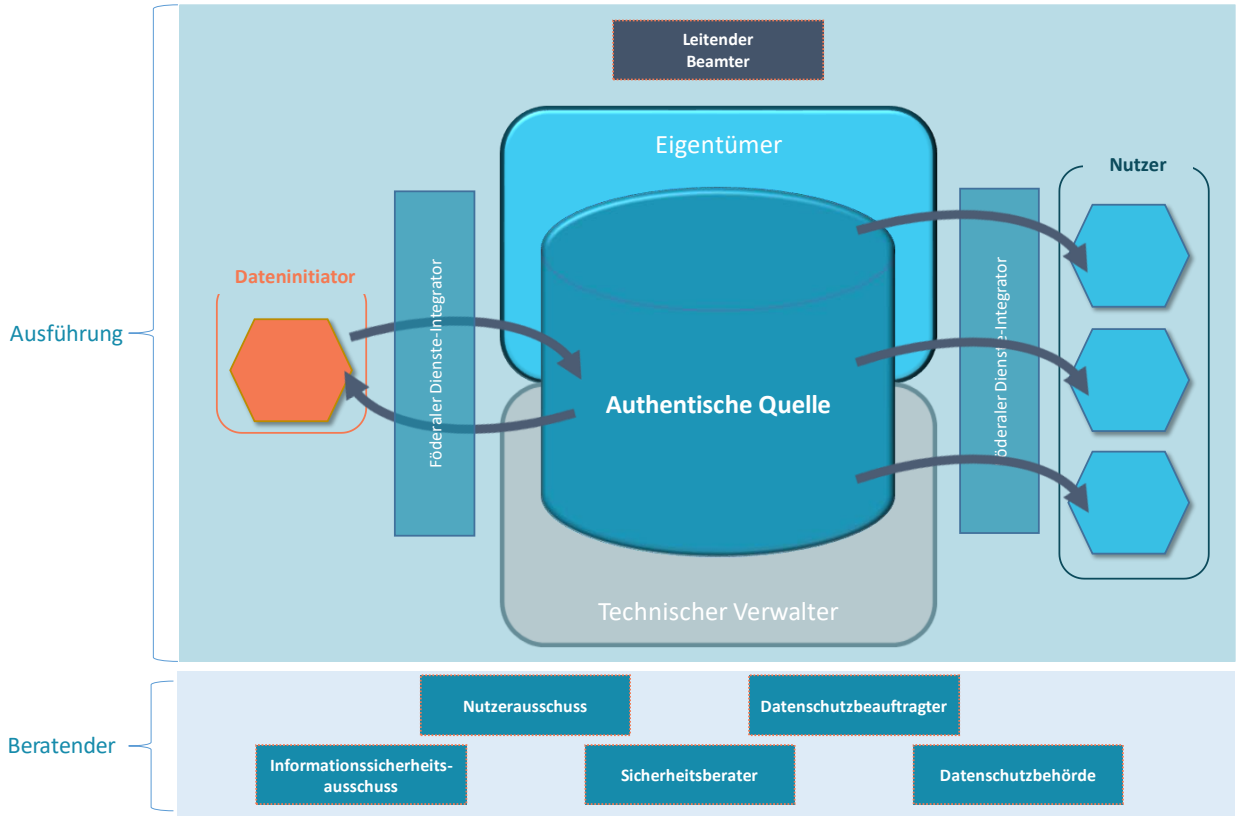
6. Wenn keine Quelle in der Liste von BOSA DT steht, müssen Sie gewährleisten, dass es keine anderen öffentlichen Dienste gibt, die ähnliche Daten speichern.

   Sie können hierfür Kontakt mit dem FÖD BOSA DT (https://dtservices.bosa.be/nl/Contact/contactformulier) aufnehmen und die Mitarbeiter fragen, ob sie wissen, ob es noch andere (nicht authentische) Quellen mit denselben Daten gibt.
   Sie können auch selbst direkt Kontakt mit anderen öffentlichen Diensten aufnehmen, um sie zu fragen, ob sie ähnliche Daten speichern und als authentische Quelle anbieten möchten.

   Wenn Sie erfahren, dass es andere Quellen mit denselben Daten gibt, müssen Sie Kontakt mit den Inhabern dieser Quellen aufnehmen, um zu vereinbaren, wer der „Inhaber“ der Daten ist.

Wenn der Inhaber einer Information oder mehrerer Daten festgestellt wurde, kann diese Instanz das Verfahren zur Anerkennung der authentischen Quelle einleiten. Ausführlichere Informationen über das Verfahren zur Anerkennung einer authentischen Quelle finden Sie in Abschnitt 3: „Wie mache ich eine authentische Quelle verfügbar?“.

2.2 Was sind die Rollen und Aufgaben für meine authentische Quelle?



Für jede authentische Quelle gibt es verschiedene Rollen, sowohl im Governance-Bereich („Lenkung“ der authentischen Quelle) als auch hinsichtlich der Durchführung.

Im Rahmen der *Durchführung* müssen immer mindestens 4 Rollen definiert sein:

- Dateninitiator
- Inhaber
- Technischer Verwalter
- Nutzer.

Außerdem wird für jede Quelle eine *Governance*-Struktur eingerichtet.

Einerseits wird für jede authentische Quelle ein *Nutzerausschuss* zusammengestellt. Es gibt nur einen einzigen Ausschuss für jede authentische Quelle. Dieser Ausschuss besteht aus den wichtigsten Interessengruppen (Vertretern der wichtigsten Nutzer, dem Inhaber, dem technischen Verwalter und den Dateninitiatoren).

Es werden auch 2 Rollen für Sicherheit und Datenschutz vorgesehen. Das sind der *Sicherheitsberater* und der *Data Protection Officer,* der immer dann bestellt werden muss, wenn die authentische Quelle personenbezogene Daten enthält. Wenn es personenbezogene Daten betrifft, können der Sicherheitsberater und der Data Protection Officer ihrerseits die Dienstleistungen der folgenden 2 Gremien in Anspruch nehmen:

- Informationssicherheitsausschuss
- Datenschutzbehörde

Das sind offizielle Instanzen, die den DPO in Bezug auf den Datenschutz und die Sicherheit der personenbezogenen Daten beraten können.

Nachstehend finden Sie eine zusammenfassende Übersicht über die typischen Tätigkeiten für jede Rolle. Die exakten Verantwortlichkeiten können für jede authentische Quelle unterschiedlich sein und müssen in einer Dienstleistungsvereinbarung zwischen den Parteien festgelegt werden (siehe Abschnitt 2.5: „Welche Absprachen können zwischen den verschiedenen Parteien getroffen werden?“).

2.2.1 Durchführung

Die Datenschutzbehörde unterscheidet 4 große Phasen bei der Verarbeitung personenbezogener Daten *(Empfehlung Nr. 09/2012 vom 23. Mai 2012, Artikel 6)*:

- Erfassung: Erhebung von Daten und diese in einem korrekten Format dokumentieren
- Validierung: Gewährleistung, dass die Daten korrekt sind
- Verwaltung: Verwaltung der Nutzung, Anwendung, Wartung und Speicherung von Daten
- Austausch personenbezogener Daten.

In der folgenden Übersicht sehen Sie, welche Rollen in diesen Phasen beteiligt sind.

	Akquisition	Validierung	Verwaltung	Austausch
Dateninitiator	X	X		X
Eigentümer	X	X	X	X
Technischer Verwalter			X	X
Nutzer				

Rolle: Dateninitiator

Beschreibung

Der Dateninitiator ist die Person, die für die Erfassung, die *Eingabe und Validierung* der *ursprünglichen (authentischen) Daten verantwortlich ist.* Der Dateninitiator fungiert als erster Ansprechpartner für Bürger und Unternehmen.

Aufgaben

- Erfassung der Daten über Bürgern und Unternehmen
- Aufnahme der fehlenden Daten in das System mithilfe offizieller Dokumente und/oder durch elektronisches Einlesen von Daten
- Korrekte Registrierung der neuen Daten
- Änderung der Daten
- Überprüfung auf Richtigkeit und Vollständigkeit
- Austausch der korrekten Datenpakete mit dem Inhaber anhand eines vorher festgelegten Verfahrens, das in einer Dienstleistungsvereinbarung mit dem Inhaber spezifiziert wird (siehe Abschnitt 2.5: „Welche Absprachen können zwischen den verschiedenen Parteien getroffen werden?“)

- Registrierung eines Auditprotokolls nach den Bestimmungen der Dienstleistungsvereinbarung.

Rolle: Inhaber

Beschreibung

Der Inhaber trägt die *Endverantwortung* für die Daten. Das bedeutet, dass der Inhaber auch die Endverantwortung für die Richtigkeit, Vollständigkeit, Verfügbarkeit und Sicherheit der Daten sowie für die *Verarbeitung* und den *Austausch* der Daten mit anderen Instanzen trägt. Eine öffentliche Einrichtung gilt als Inhaber einer authentischen Information, wenn sie folgende Bedingungen erfüllt:

- Der öffentliche Dienst hat einen gesetzlichen Auftrag zur Erhebung und Verarbeitung der Daten.
- Der öffentliche Dienst kann, besser als andere öffentliche Dienste, leichter auf die Daten zugreifen und hat bereits die meisten Daten erhoben.

Aufgaben

- Erfassung der Daten über den Dateninitiator anhand eines vorher festgelegten Verfahrens, das in einer Dienstleistungsvereinbarung mit dem Dateninitiator spezifiziert wird (siehe Abschnitt 2.5: „Welche Absprachen können zwischen den verschiedenen Parteien getroffen werden?“)
- Erstellung der Strategie zur Aktualisierung der Daten, in Zusammenarbeit mit dem Dateninitiator.
- Endverantwortung für die Richtigkeit, Vollständigkeit, Verfügbarkeit und Sicherheit der Quelle
- Austausch der korrekten Datenpakete mit anderen Instanzen anhand eines vorab festgelegten Verfahrens (siehe Abschnitt 3: „Wie mache ich eine authentische Quelle verfügbar?“)
- Registrierung eines Auditprotokolls nach den Bestimmungen der Dienstleistungsvereinbarung

Rolle: Technischer Verwalter

Beschreibung

Der technische Verwalter der (authentischen) Daten ist die Instanz, die für die Erarbeitung der *technischen Modalitäten* im Zusammenhang mit der Erfassung, Speicherung und Wartung der Daten und die Übermittlung von Daten an ihren Dienste-Integrator verantwortlich ist. Die Verbindung mit anderen Integratoren oder Instanzen wird vom gekoppelten Dienste-Integrator gesteuert. Der Inhaber der Quelle ist für die technischen Modalitäten verantwortlich.

Aufgaben

Der technische Verwalter hat unter anderem die folgenden Aufgaben:

1. Festlegung und Einrichtung der technischen Struktur der Quelle
2. Festlegung und Einrichtung eines *Datenmodells*
3. *Festlegung* der *Schnittstellen* zur authentischen Quelle
4. *Umsetzung* in die korrekte *Struktur* der Daten (beispielsweise SD oder XML)
5. Korrekte *Anreicherung* der *Daten* mit anderen Daten des Inhabers, falls dies mit einem System durchgeführt wird

Die Verbindung mit anderen Integratoren oder Instanzen wird vom gekoppelten Dienste-Integrator gesteuert.

Rolle: Nutzer

Jede natürliche oder juristische Person, einschließlich von Unternehmen, Einrichtungen, Vereinigungen und allen Abteilungen der Behörde selbst, die berechtigt sind, die authentischen Daten einzusehen und für eigene Zwecke zu verwenden.

Eine Berechtigung kann eine Erlaubnis des zuständigen Organs (Informationssicherheitsausschuss oder Minister des Innern) sein oder auf einem Protokoll basieren, das zwischen dem Inhaber und dem Nutzer erstellt wurde.

Beispiele:

Quelle	Dateninitiator(en)	Inhaber	Technischer Verwalter
Nationalregister	• Gemeinden	• FÖD Inneres	• FÖD Inneres
Zentrale Datenbank der Unternehmen	• Unternehmensgericht • Unternehmensschalter • LSS	• FÖD Wirtschaft	• FÖD Wirtschaft
Ländercodes	• GD Statistik	• FÖD Auswärtige Angelegenheiten	• FÖD Wirtschaft

2.2.2 Governance

Rolle: Nutzerausschuss

Beschreibung

Der Nutzerausschuss handelt als übergreifendes Organ, das für das *gute Funktionieren* der Datenerfassung und des Datenaustausches verantwortlich ist. Er sorgt dafür, dass alle wichtigen *Interessengruppen* die Funktions- und Verfahrensweisen der authentischen Quelle mitbestimmen können. Dies entspricht der Empfehlung der Datenschutzbehörde (Empfehlung Nr. 09/2012 vom 23. Mai 2012). Für jede authentische Quelle muss ein Nutzerausschuss eingerichtet werden.

Aufgaben

1. Abstimmung in Bezug auf gemeinsame Verpflichtungen, die in die Dienstleistungsvereinbarungen zwischen den beteiligten Parteien aufgenommen wurden.
2. Abstimmung in Bezug auf die Nutzung der verschiedenen Systeme, die für die Erfassung, die Validierung, die Verwaltung und den Austausch der Daten mit den beteiligten Parteien verwendet werden.

3. Beratung zwecks Optimierung des Prozesses von der Datenerfassung bis hin zum Datenaustausch.
4. Abstimmung über die Zusammenarbeit zwischen den Interessengruppen oder über die Funktionsweise der verwendeten Systeme.

Rolle: Data Protection Officer (DPO)

Beschreibung

Ein Data Protection Officer wird als *Experte* für die Datenverarbeitung im Hinblick auf den *Datenschutz* und die *Sicherheit* der *personenbezogenen Daten bestellt.*

Eine öffentliche Einrichtung ist dazu verpflichtet, einen DPO nach Artikel 37, 1, a) der Europäischen Verordnung 2016/679 zu bestellen.

Eine private Körperschaft, die personenbezogene Daten für Rechnung einer Föderalbehörde verarbeitet oder die personenbezogene Daten von einer Föderalbehörde erhält, bestellt einen Datenschutzbeauftragten, wenn die Verarbeitung dieser Daten ein hohes Risiko beinhalten kann.

Aufgaben

Der DPO hat – in Übereinstimmung mit der Datenschutz-Grundverordnung – folgende Aufgaben:

1. *Unterrichtung* und *Beratung* der Datenverwalter und Datenverarbeiter (Dateninitiatoren, Inhaber und technische Verwalter)
   a. Die Daten dürfen nur für den Zweck verwendet werden, für den sie erhoben wurden.
   b. Es dürfen nicht mehr Daten als für den Erhebungszweck erforderlich gespeichert werden.
   c. Die Daten dürfen nicht länger als erforderlich gespeichert werden.
2. *Überprüfung* auf Einhaltung der Datenschutzmaßnahmen, die von den europäischen und belgischen Rechtsvorschriften im Datenschutzbereich auferlegt wurden.
3. *Erster Ansprechpartner* in Bezug auf die Sicherheit und den Datenschutz personenbezogener Daten.
4. Verwaltung der Datenverarbeitungsformalitäten, wie die Erstellung einer *Protokollvereinbarung*. Die Sicherheitsberater beider Parteien erstellen eine Vereinbarung über den Austausch von Daten. Bei Streitfragen kann man sich an den Informationssicherheitsausschuss wenden.

Rolle: Sicherheitsberater

Beschreibung

Ein Sicherheitsberater erteilt Ratschläge über alle Informationssicherheitsaspekte und sorgt für die betreffende Betreuung. Ein Sicherheitsberater wird als *Experte* für die Datenverarbeitung im Hinblick auf *die Sicherheit* der *personenbezogenen Daten bestellt.*

Aufgaben

1. *Unterrichtung* und *Beratung* der Datenverwalter und Datenverarbeiter
2. Gewährleistung *in Rücksprache* mit dem *technischen Verwalter,* dass die *Erfassung, die Validierung, die Verwaltung und der Austausch* der Daten auf *sichere* Art und Weise erfolgen.

Datenschutzbehörde

Beschreibung

Die Datenschutzbehörde ist die belgische Behörde, die den *Datenschutz* bei der Verarbeitung personenbezogener Daten überwacht. Die Datenschutzbehörde ist seit dem Inkrafttreten der Datenschutz-Grundverordnung im Mai 2018 die Nachfolgerin der Ausschuss für den Schutz des Privatlebens (Gesetz vom 3. Dezember 2017 zur Schaffung der Datenschutzbehörde).

Aufgaben

- Beratung in Bezug auf Datenschutz und Sicherheit bei der Verarbeitung personenbezogener Daten

Informationssicherheitsausschuss (ISA)

Beschreibung

Der Informationssicherheitsausschuss ist ein unabhängiges Gremium, das bestimmt, welche *personenbezogenen Daten geteilt* werden dürfen und unter welchen *Sicherheitsbedingungen* dies zu erfolgen hat.

Der ISA besteht aus einer Kammer für die soziale Sicherheit und Gesundheit und einer Kammer für die Föderalbehörde.

(Gesetz vom 5. September 2018: *Loi instituant le comité de sécurité de l'information et modifiant diverses lois concernant la mise en oeuvre 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*)

Achtung! Der Zugriff auf Daten des Nationalregisters oder auf Daten im Sinne von Artikel 5, § 2 des Gesetzes über das Nationalregister sowie die Verwendung der Nationalregisternummer müssen beim FÖD Inneres beantragt werden (Artikel 5 des Gesetzes vom 8. August 1983 zur Organisation eines Nationalregisters der natürlichen Personen).

Aufgaben

- Erteilung einer Genehmigung für den Austausch personenbezogener Daten zwischen der authentischen Quelle und den Nutzern.

7. Zuweisung der Durchführungsrollen der authentischen Quelle an spezifische (Teile von) Organisationen:
   - Dateninitiator(en)
   - Inhaber
   - Technischer Verwalter
   - Nutzer.

8. Festlegung, wer die Rolle als Sicherheitsberater und DPO (falls erforderlich) erfüllen wird.

9. Zusammenstellung des Nutzerausschusses und Festlegung seiner Arbeitsweise (Häufigkeit, Tagesordnung usw.).

10. Gewährleistung, dass die Absprachen über die Aufgaben jeder Partei deutlich sind und in Dienstleistungs- und Nutzervereinbarungen festgelegt werden (siehe Abschnitt 2.5: „Welche Absprachen können zwischen den verschiedenen Parteien getroffen werden?“).

2.3 Wie wähle ich ein Datenmodell für meine authentische Quelle aus?

Öffentliche Einrichtungen dürfen Daten nur ein einziges Mal bei Bürgern und Unternehmen anfordern *(Only-once-Gesetz, 5. Mai 2014).* Danach werden diese Daten zwischen den verschiedenen öffentlichen Diensten *zwecks Wiederverwendung geteilt*.

Eine authentische Quelle enthält nur *Rohdaten*, ohne irgendeine Form von Geschäftslogik. Die Auslegung der Daten und die Hinzufügung spezieller Geschäftslogik werden außerhalb der Quelle vom Inhaber oder den Dienste-Integratoren durchgeführt. Der Inhaber der Quelle kann außer den generischen Daten eventuell zusätzliche Dienstleistungen mit Geschäftslogik anbieten.

Deshalb ist es wichtig, dass das „Datenmodell“ der authentischen Quelle gut beschrieben ist und dass dies auch veröffentlicht wird, damit die anderen öffentlichen Dienste dies berücksichtigen können.

Das Datenmodell beschreibt, *wie die Daten in einer Datenquelle gespeichert werden* und wie sich diese Daten in Bezug aufeinander verhalten. Das Datenmodell wird normalerweise von einem Funktionsanalysten oder einem IT-Architekten erstellt, bevor die Datenquelle entwickelt wird.

Es empfiehlt sich, die folgenden Elemente in der Beschreibung des Datenmodells zu bewerten:

1. Gültigkeitsfrist
2. Inhalt der Daten
3. Nomenklatur: Sprachgebrauch, Namensgebungen, Abkürzungen usw.
4. Technische Anforderungen
5. Einmaligkeit

Daneben können – abhängig von den Daten und den Bedürfnissen Ihrer Quelle – noch viele andere Elemente aufgenommen werden.

11. Ermitteln Sie die Erwartungen Ihrer Interessengruppen: Welche Informationen über Ihre Daten *benötigen sie?*

12. Bitten Sie Ihren IT-Architekten oder Analysten der Datenquelle, die Beschreibung des Datenmodells in Abhängigkeit von den Fragen zu erstellen, die Sie von Ihren Interessengruppen erhalten haben. Orientieren Sie sich an Interoperabilitätsrahmen (wie das European Interoperability Framework), um eine maximale Kompatibilität und einen optimalen Austausch zu ermöglichen.

2.4 Warum und wie erstelle ich ein Auditprotokoll und einen Audit Trail in Bezug auf den Datenschutz?

2.4.1 Datenschutz Auditprotokoll

Eine authentische Quelle enthält eindeutige Daten, die mit allen Behörden geteilt und in offiziellen Verfahren und Nachrichten der Behörden verwendet werden. Deshalb ist es wichtig, dass immer überprüft werden kann, wann und wie Daten verwendet und geändert wurden und dass diese Informationen *geltend gemacht werden können*.

Daher müssen die Zweckbestimmung und die Verhältnismäßigkeit der Daten in einer authentischen Quelle immer gewährleistet sein:

- Die *Zweckbestimmung* umfasst einen bestimmten, ausdrücklich beschriebenen und genehmigten Zweck.
- Die *Verhältnismäßigkeit* bedeutet, dass die Daten in Anbetracht des Zwecks, für den sie erhalten oder weiterverarbeitet werden, ausreichend, sachdienlich und nicht übermäßig sein dürfen. Die Daten dürfen auch nicht länger als für den genehmigten Zweck unbedingt erforderlich gespeichert werden.

Um zu überprüfen, dass jede authentische Quelle die *anwendbaren Rechtsvorschriften einhält*, müssen alle beteiligten Parteien ein Datenschutz Auditprotokoll erstellen.

Ein *Datenschutz Auditprotokoll* ist ein Protokoll, das automatisch vom System erzeugt wird und Informationen über die *Abfrage* oder die *Erstellung, Änderung und Löschung* von *Daten* umfasst. Dieses Protokoll wird von jedem System erstellt, das an der Einrichtung und Durchführung der authentischen Quelle beteiligt ist. Diese Informationen sorgen dafür, dass man für jedes System immer überprüfen kann, welche Art von Abfrage oder Änderung von Daten durchgeführt wurde. Im Protokoll werden normalerweise die folgenden Informationen über die Abfrage oder die Änderung erfasst:

1. Die eindeutige Nutzer-ID (wer)
2. Datum und Uhrzeit (wann)
3. Art der Abfrage/Änderung
4. alter Wert und neuer Wert der Information (was).

Außer diesen Informationen müssen die beteiligten Parteien festlegen, welche anderen Informationen noch in das Datenschutz Auditprotokoll aufzunehmen sind.

Ein Datenschutz Auditprotokoll muss 10 Jahre verfügbar bleiben. Weil die Daten im Datenschutz Auditprotokoll auch personenbezogene Daten sein können, müssen diese hinterher gelöscht werden. Für jede authentische Quelle muss jedoch individuell festgelegt werden, wie lange die Daten verfügbar bleiben müssen, um die rechtlichen Anforderungen zu erfüllen.

2.4.2 Datenschutz Audit Trail

Durch Gruppierung der Auditprotokolle aller Systeme der Parteien in der Kette (Nutzerorganisation, Dienste-Integrator, Quellenverwalter) kann ein Datenschutz Audit Trail rekonstruiert werden, der angibt, welcher Endbenutzer zu welchem Zeitpunkt und in welchem Kontext eine besondere Abfrage durchgeführt hat.

Dieser Audit Trail sorgt dafür, dass die Transaktionen, die über den Dienste-Integrator durchgeführt werden, rekonstruiert werden können, sodass die gesetzliche Verpflichtung in Bezug auf

personenbezogene Daten eingehalten werden kann. Jeder Partner in der Kette (Dateninitiator, Inhaber und Nutzer) bleibt jedoch für die Auditprotokolle auf seinen eigenen Systemen verantwortlich.

13. Besprechen Sie mit dem Dateninitiator, dem Inhaber und dem Nutzer der authentischen Quelle, wie die Auditprotokolle erstellt werden, welche Informationen darin gespeichert werden und wie ein Audit Trail erstellt werden kann. Beachten Sie dabei die folgenden Punkte:

- **Sicherheit**: Sorgen Sie dafür, dass jedes Datenschutz Auditprotokoll gesichert ist und weder geändert, gelöscht noch deaktiviert werden kann. Nur ein privilegierter Nutzer (beispielsweise ein Administrator) des Systems kann die Daten im Auditprotokoll ändern, löschen oder deaktivieren, wobei er ein kontrolliertes Verfahren anwendet. Diese Aktionen werden auch vom System gespeichert.

- **Verfügbarkeit**: Der Audit Trail muss bis zu 10 Jahre rekonstruiert werden können (sofern es keine anderen rechtlichen Anforderungen gibt). Im Falle einer Untersuchung müssen die Daten auf Anfrage innerhalb von 24 Stunden übermittelt werden können. Die Daten im Datenschutz Auditprotokoll müssen gedruckt oder exportiert werden können. Die Daten des Audit Trails müssen nach Ablauf der gesetzlichen Aufbewahrungsfrist gelöscht werden.

- **Datenschutz**: Im Idealfall wird dem Bürger *auch die Möglichkeit* geboten, *festzustellen,* wer *seine Daten* für welchen Zweck in den vergangenen Monaten abgefragt hat (beispielsweise über eine Webanwendung wie „Meine Akte“ für das Nationalregister). Der Inhaber der authentischen Quelle kann selbst das Verfahren und die Infrastruktur wählen, mit denen er dies auf gesicherte Weise und mit Respekt vor dem Datenschutz durchführen kann.

Weitere rechtliche und technische Angaben zur Erstellung eines Datenschutz Audit Trails finden Sie auch in der Anleitung „Het opzetten van een audit trail: Handleiding voor fedict ketenpartners“ << LINK >>.

2.5 Welche Absprachen können zwischen den verschiedenen Parteien getroffen werden?

Um zufriedene Nutzer zu haben, ist es wichtig, die Erwartungen im Voraus korrekt zu ermitteln und diese so deutlich wie möglich in formellen Absprachen festzulegen. Die Absprachen können in Nutzervereinbarungen oder in Dienstleistungsvereinbarungen (Service Level Agreement – SLA) aufgenommen werden.

In der Nutzervereinbarung werden *die Rechte und Pflichten* zur Nutzung der authentischen Quelle festgelegt. Die Nutzervereinbarung umfasst normalerweise folgende Daten:

- Beschreibung des Dienstes
- Bedingungen zur Nutzung des Dienstes (Kosten, Zwecke, Volumen usw.)
- Sicherheitsabsprachen (beispielsweise Genehmigungen, Audit Trail usw.)

Ein Beispiel für eine Nutzervereinbarung ist die „Nutzervereinbarung FSB“ (verfügbar unter https://dtservices.bosa.be/fr/services/fsb/demande-dun-service-web-fsb-ou-dun-certificat-fsb/je-demande-dacceder-un-service-web)

Eine *Dienstleistungsvereinbarung* ist eine *Vereinbarung,* um den *Informationsaustausch* zwischen den beiden beteiligten Parteien zu koordinieren. Diese Vereinbarung kann in die Nutzervereinbarung aufgenommen oder separat abgeschlossen werden. Eine Dienstleistungsvereinbarung umfasst einige Bedingungen und Komponenten, an die sich beide Parteien halten. Eine Dienstleistungsvereinbarung kann zwischen dem Inhaber und dem Nutzer erstellt werden, oder zwischen dem Inhaber und der Partei die für die Zurverfügungstellung der Quelle verantwortlich ist (Dienste-Integrator).

Idealerweise sind die folgenden Elemente in einer Dienstleistungsvereinbarung enthalten:

1. **Art der Daten**
   - Name der Daten
   - Kurze Beschreibung der Daten
   - Zweck für die Speicherung dieser Daten.
2. **Verfahren**
   - Verfahren, die sicherstellen, dass die typischen Merkmale (Richtigkeit, Vollständigkeit, Sicherheit und Verfügbarkeit) einer authentischen Quelle bei der Erfassung, der Validierung und dem Austausch der authentischen Daten gewährleistet sind;
   - Verfahren, die gewährleisten, dass eine Berichtigung oder Aktualisierung von einer Information anhand eines vorher festgelegten Verfahrens validiert und angepasst werden kann.
3. **Rollen und Aufgaben**
   - Rolle des Dateninitiators
   - Rolle des Inhabers
   - Rolle des technischen Verwalters
   - Rolle des Nutzerausschusses
   - (siehe Abschnitt 2.2: „Was sind die Rollen und Aufgaben für meine authentische Quelle?“)
4. **Datenschutz Auditprotokoll**
   - Festlegung, wer für die Registrierung des Datenschutz Auditprotokolls für jede beteiligte Partei und für die Rekonstruktion des Audit Trails bei einer Abfrage verantwortlich ist. (siehe Abschnitt

2.4: „Warum und wie erstelle ich ein Auditprotokoll und einen Audit Trail in Bezug auf den Datenschutz?“).

5. Technische Anforderungen

- Änderungs- und Release-Management;
  - Festlegung des Verfahrens in Bezug auf Änderungsvorschläge
  - Wartung der Systeme (beispielsweise vorher festgelegte Termine für Updates oder Upgrades)
- Verfügbarkeit der Systeme (ausschließlich 24/7 oder nur während der Geschäftszeiten);
- Möglichkeiten zur Herstellung von Verbindungen mit den Systemen (beispielsweise webbasiert);
- Leistungsfähigkeit der Systeme (beispielsweise Reaktionszeit in x Millisekunden);
- Kapazitätsbeschränkungen der Systeme (beispielsweise Anzahl aktiver Nutzer pro Minute);
- Follow-up von Meldungen von Störungen in den Systemen und vorgesehene Reaktionszeit (beispielsweise Störungen mit hoher Priorität müssen innerhalb von 4 Stunden behoben werden).

Die obenstehenden Elemente sind jedoch lediglich als Hinweis gedacht. Für weitere Ratschläge über wichtige Aspekte, die in diese Vereinbarung aufgenommen werden müssen, kann man sich an den Nutzerausschuss wenden.

Eine Vorlage für eine Dienstleistungsvereinbarung finden Sie unter <<LINK TOE TE VOEGEN> >

14. Fragen Sie den Nutzerausschuss, welche Elemente (Verfahren, Aufgaben usw.) festgelegt werden müssen und sorgen Sie dafür, dass diese klar und vollständig aufgenommen werden.

3 Wie mache ich eine authentische Quelle verfügbar?

In diesem Abschnitt erhalten Sie einen besseren Einblick in die Bereitstellung einer authentischen Quelle. Diesbezüglich müssen die folgenden zwei Schritte durchgeführt werden:

1. Anerkennung der Quelle als authentische Quelle: In den vorigen Abschnitten wurde bereits erläutert, was eine authentische Quelle ist und wie Sie diese erstellen müssen. In diesem Abschnitt wird ausführlicher darauf eingegangen, wie eine authentische Quelle anerkannt werden kann.
2. Außerdem muss eine Quelle zugänglich gemacht werden, damit die Daten von diesbezüglich autorisierten Nutzern abgerufen werden können.

3.1 Wie kann ich meine Quelle in die veröffentlichte Liste der authentischen Quellen des föderalen Dienste-Integrators aufnehmen lassen?

Das Verfahren zur Veröffentlichung einer authentischen Quelle kann auf zwei verschiedene Weisen durchgeführt werden.

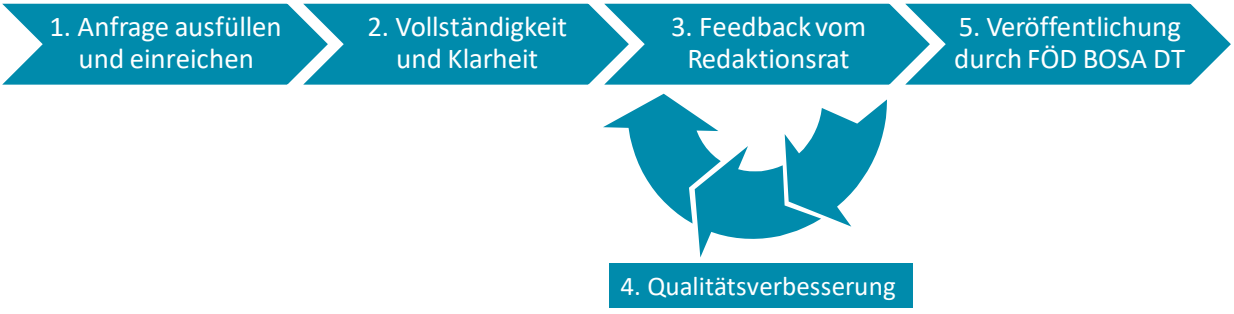
3.1.1 Veröffentlichung als authentische Quelle durch Königlichen Erlass

Eine Datenquelle kann als authentische Quelle anerkannt werden, wenn hierfür ein Königlicher Erlass oder ein Gesetz genehmigt wird. Nach Veröffentlichung im Belgischen Staatsblatt kann der FÖD BOSA die Daten Ihrer authentischen Quelle in die Liste der authentischen Quellen aufnehmen.

3.1.2 Veröffentlichung als authentische Quelle durch den Redaktionsausschuss

Hinweis: Dieses Verfahren wurde noch nicht endgültig festgelegt. Alle Informationen in diesem Abschnitt können noch geändert werden. Bei etwaigen Änderungen wird der FÖD BOSA DT eine neue Fassung dieses Dokuments veröffentlichen.

Der Koordinierungsausschuss des föderalen Dienste-Integrators, in dem alle beteiligten Behörden vertreten sind, hat einen „Redaktionsausschuss für authentische Quellen“ eingerichtet. Dieser Redaktionsausschuss wurde damit beauftragt, zu bewerten, ob potenzielle Datenquellen die Anforderungen einer authentischen Quelle erfüllen, und diese in die Liste der authentischen Quellen aufzunehmen.



1. Für eine Veröffentlichung der authentischen Quelle durch den föderalen Dienste-Integrator füllen Sie die Vorlage für die Veröffentlichung aus (siehe Abschnitt 4: „Antragsformular Veröffentlichung“). Der Antrag wird beim FÖD BOSA DT unter https://dtservices.bosa.be/fr/Contact/formulaire_de_contact eingereicht.

2. Der föderale Dienste-Integrator stimmt sich mit dem Antragsteller ab, um zu gewährleisten, dass der Antrag klar und vollständig ist.
3. Der föderale Dienste-Integrator leitet den Antrag an die Mitglieder des Redaktionsausschusses weiter. Die Mitglieder des Redaktionsausschusses haben 3 Wochen Zeit (zu bestätigen), um Feedback zu geben. Wenn kein Feedback erhalten wird, wird der Antrag genehmigt.
4. Der föderale Dienste-Integrator unterstützt den Antragsteller, um die Qualität der authentischen Quelle zu verbessern.
5. Bei Genehmigung des Antrags wird der Inhaber informiert. Der föderale Dienste-Integrator nimmt die Quelle in die Liste der authentischen Quellen auf und erstellt Links zu den folgenden Informationen des Inhabers über die authentische Quelle, die dieser veröffentlichen muss:

    1. *Merkmale* der Information wie Inhalt, Art der Registrierung, Änderungshäufigkeit und technische Spezifikationen;
    2. Verfahren für die *Registrierung*;
    3. *Verwaltung* der Information und *Verteilung der Aufgaben* in jeder Registrierungsphase;
    4. Verfahren für die *Zugänglichkeit* der Information;
    5. Verfahren, um die *Richtigkeit*, die *Vollständigkeit*, die *Sicherheit* und *Verfügbarkeit* der Information dauerhaft zu gewährleisten;
    6. *Transparente Absprachen* mit dem öffentlichen Dienst, der die Information erhalten möchte;
    7. Verfahren für die *Rückmeldung* von Fehlern in der Information und für die *Berichtigung* der Information;
    8. Rücksprache im Hinblick auf die Verbesserung der *Qualität*, der *Verfügbarkeit* und der Nutzung *der* Information;
    9. Beschreibung der Art und Weise, wie die *betroffene Person* ihre *Rechte* in Bezug auf ihre personenbezogenen Daten *ausüben* kann.

3.2 Wie mache ich meine Quelle verfügbar?

Der Inhaber und der technische Verwalter der authentischen Quelle legen die Art und Weise fest, wie die authentische Quelle zugänglich gemacht wird. Diese Entscheidung hängt von der Art der Daten ab, die angeboten werden, sowie von der Art und Weise, wie der Nutzer diese Daten anwendet.

Über den föderalen Dienste-Integrator kann die Zurverfügungstellung effizient erfolgen und wird gewährleistet, dass der Zugriff auf die authentischen Quellen und der schnelle Datenaustausch auf homogene und sichere Art und Weise erfolgen.

Nachstehend werden einige Möglichkeiten angegeben, um eine authentische Quelle verfügbar zu machen:

1. Webservice: über die REST- oder SOAP-Technologie
2. File Transfer Protocol (FTP)
3. HTML
4. Excel
5. Veröffentlichung auf einer Website
6. …

Außerdem müssen Sie eine Auswahl bezüglich der Häufigkeit (Echtzeit vs. Stapelverarbeitung) der Datenverarbeitung und der Verfügbarkeit ihrer Quelle (dauerhaft vs. periodisch) treffen. Bei diesen

Entscheidungen kann sich der Inhaber vom Koordinierungsausschuss, dem Sicherheitsberater und dem technischen Verwalter beraten lassen. Der technische Verwalter muss hinterher die erforderliche technologische Unterstützung für die Entscheidungen bezüglich der authentischen Quelle gewähren.

Üblicherweise werden die folgenden Tätigkeiten in die Zurverfügungstellung der authentischen Quelle aufgenommen:

- Erstellung der Funktionsbeschreibung der Quelle
- Festlegung von Testfällen
- Einrichtung einer Testumgebung, eventuell mit anonymisierten Daten
- Dokumentation der funktionellen und technischen Fehlercodes.

Für weitere Informationen über diese Tätigkeiten können Sie Kontakt mit dem FÖD BOSA DT aufnehmen.

4 Antragsformular Veröffentlichung

Mit diesem Antragsformular können Sie alle Daten Ihrer potenziellen authentischen Quelle angeben. Sie müssen diese Checkliste auch verwenden, um Ihren Veröffentlichungsantrag einzureichen (siehe Abschnitt 3.1.2: „Veröffentlichung als authentische Quelle durch den Redaktionsausschuss“).

1. Geschäftsszenario

Beschreiben Sie kurz den Zweck Ihrer authentischen Quelle und geben Sie die potenziellen Nutzer an, die diese Daten abrufen können.

2. Gesetzlicher Auftrag

Geben Sie an, welche Rechtsgrundlage, Verordnung oder sonstigen Informationen auf Ihre Organisation anwendbar sind, aus denen Sie ableiten, dass Sie den gesetzlichen Auftrag haben, um diese Daten zu erheben und in einer authentischen Quelle zu speichern.

3. Beschreibung der authentischen Quelle

Geben Sie die Daten an, die Sie in der authentischen Quelle speichern werden.

4. Garantie hinsichtlich Richtigkeit und Vollständigkeit

Beschreiben Sie, wie Sie gewährleisten, dass Ihre Daten vollständig und richtig sind, und wie Sie dies auch zukünftig gewährleisten können.

Gibt es ein Feedback-Verfahren (beispielsweise Meldestelle), um Fehler zu berichtigen?

5. Rollen

Geben Sie die Personen an, denen die folgenden Rollen zugewiesen werden:

Dateninitiator(en)	*Wer wird, falls erforderlich, die Daten eingeben und ändern?*
Inhaber	*Wer wird der Inhaber Ihrer authentischen Quelle?*
Technischer Verwalter	*Wer wird die technischen Modalitäten Ihrer authentischen Quelle festlegen und überwachen?*
Nutzer	*Wer sind die potenziellen Nutzer Ihrer authentischen Quelle?*
Nutzerausschuss	*Wie wird der Nutzerausschuss zusammengestellt?*
Data Protection Officer	*Welche Person wird als DPO für Ihre authentische Quelle auftreten?*
Sicherheitsberater	*Welche Person wird als Sicherheitsberater für Ihre authentische Quelle auftreten?*

6. Datenschutz Auditprotokoll und Audit Trail

Bitte geben Sie an, dass Sie die folgenden Aspekte des Datenschutz Auditprotokolls berücksichtigen.

Jedes System, das an meiner authentischen Quelle beteiligt ist, hat ein Datenschutz Auditprotokoll.	*Ja/Nein*
Die Datenschutz Auditprotokolle aller Systeme werden 10 Jahre lang gespeichert.	*Ja/Nein*
Die Daten der Datenschutz Auditprotokolle können auf Anfrage innerhalb von 24 Stunden übermittelt werden.	*Ja/Nein*

7. Datenmodell

Geben Sie kurz die Erwartungen Ihrer Interessengruppen an: Welche Informationen über Ihre Daten benötigen sie?

Geben Sie für die oben aufgelisteten Punkte konkrete und einzige Datenelemente an.

8. Dienstleistungsvereinbarung

Wurde eine Dienstleistungsvereinbarung zwischen allen beteiligten Parteien vorgesehen? Wenn nicht, begründen Sie kurz, warum keine Dienstleistungsvereinbarung erstellt wurde.

Wurde der Nutzerausschuss in Bezug auf die Elemente zurate gezogen, die in die Dienstleistungsvereinbarung(en) aufgenommen werden müssen?

Was muss in den Dienstleistungsvereinbarung(en) bezüglich der Art der Daten beschrieben werden?

Welche technischen Anforderungen müssen in die Dienstleistungsvereinbarung(en) für den Datenaustausch aufgenommen werden?

5 Begriffsbestimmungen

Authentische Quelle	*„Eine authentische Quelle ist eine Datenbank, in der authentische Daten gespeichert sind.“ (Gesetz über die Schaffung und Organisation eines föderalen Dienste-Integrators, 15. August 2012, Artikel 2).* Diese Daten werden als die ursprünglichen Daten anerkannt und gelten daher als zuverlässigste Quelle. Authentische Quellen sorgen dafür, dass Daten über eine Person oder ein Unternehmen nur einmal erhoben werden. *Ausführliche Informationen über die authentischen Quellen und Daten finden Sie in Kapitel 1.*
Authentische Daten	*„Das sind Daten, die von einer Instanz gesammelt und in einer Datenbank verwaltet werden und als einzige und ursprüngliche Daten bezüglich der betreffenden Person oder Rechtstatsache gelten, so dass dieselben Daten nicht mehr von anderen Instanzen gesammelt werden müssen.“ (Gesetz über die Schaffung und Organisation eines föderalen Dienste-Integrators, 15. August 2012, Artikel 2).* *Ausführliche Informationen über die authentischen Quellen und Daten finden Sie in Kapitel 1.*
Koordinierungsausschuss (des föderalen Dienste-Integrators)	*„Der Koordinierungsausschuss berät den föderalen Dienste-Integrator über:* 1. *den möglichen Zugang zu Datenbanken oder authentischen Quellen über den föderalen Dienste-Integrator,* 2. *die mögliche Anpassung der ausgewählten authentischen Quellen, sodass nach Möglichkeit nur authentische Daten zugänglich gemacht werden,* 3. *die Benutzung von Verweisen zu authentischen Daten in der authentischen Quelle, was Daten betrifft, die sich ganz oder teilweise mit authentischen Daten in einer authentischen Quelle überschneiden,* 4. *das Erstellen einer Regelbank für eine oder mehrere Datenbanken,* 5. *die Aufteilung der Verantwortlichkeit zwischen dem föderalen Dienste-Integrator, den teilnehmenden öffentlichen Diensten und den anderen Dienste-Integratoren, unter Berücksichtigung der Befugnisse, die ihnen durch vorliegendes Gesetz übertragen werden.“*

	(Gesetz über die Schaffung und Organisation eines föderalen Dienste-Integrators, 15. August 2012, Artikel 27, §1).
Datenmodell	Das Datenmodell beschreibt, wie die Daten in einer Datenquelle gespeichert werden, und wie sich diese Daten in Bezug aufeinander verhalten. Das Datenmodell wird normalerweise von einem Funktionsanalysten oder einem IT-Architekten erstellt, bevor die Datenquelle entwickelt wird. *Ausführliche Informationen über ein Datenmodell finden Sie in Kapitel 2.3.*
Data Protection Officer (DPO)	Die Datenschutz-Grundverordnung vom 25. Mai 2018 verpflichtet alle öffentlichen Einrichtungen, einen Data Protection Officer zu bestellen. Der DPO wird als Experte für die Datenverarbeitung im Hinblick auf den Datenschutz und die Sicherheit der personenbezogenen Daten in Übereinstimmung mit der Datenschutz-Grundverordnung vom 25. Mai 2018 bestellt. *Ausführliche Informationen über den DPO finden Sie in Kapitel 2.2.2.*
Dienste-Integrator	*Ein Dienste-Integrator ist eine Instanz, die durch oder aufgrund des Gesetzes auf einer bestimmten Befugnisebene oder in einem bestimmten Sektor mit der Dienste-Integration beauftragt ist.“* (Gesetz über die Schaffung und Organisation eines föderalen Dienste-Integrators, 15. August 2012, Artikel 2). Die Dienste-Integration ist die Organisation eines Austauschs elektronischer Daten zwischen Instanzen und die integrierte Bereitstellung dieser Daten. Es gibt 3 föderale Dienste-Integratoren: - FÖD BOSA DG Digitale Transformation (vorher Fedict), - e-Health, - Zentrale Datenbank der sozialen Sicherheit.
Inhaber	Der Inhaber ist eine der erforderlichen Rollen zur Verwaltung einer authentischen Quelle. Der Inhaber trägt die Endverantwortung für die Daten. Das bedeutet, dass der Inhaber auch die Endverantwortung für die Richtigkeit, Vollständigkeit und Verfügbarkeit der Daten sowie die Verarbeitung und den Austausch der Daten mit anderen Instanzen trägt.

	Ausführliche Informationen über die Rollen für die Verwaltung einer authentischen Quelle finden Sie in Kapitel 2.2.
Fedict-Gesetz	„Das Gesetz vom 15. August 2012 über die Schaffung und Organisation eines föderalen Dienste-Integrators“ ist allgemein als das Fedict-Gesetz bekannt. Der FÖD BOSA DG DT (vorher Fedict) wurde darin als Dienste-Integrator mit dem Auftrag bestellt, den Datenaustausch zwischen einerseits den teilnehmenden öffentlichen Diensten (d. h. allen föderalen öffentlichen Diensten und Einrichtungen, einschließlich derer, die unter die soziale Sicherheit fallen) untereinander und andererseits zwischen den teilnehmenden öffentlichen Diensten und den anderen Dienste-Integratoren zu vereinfachen und zu optimieren.
Nutzer	Jede natürliche oder juristische Person, einschließlich von Unternehmen, Einrichtungen, Vereinigungen und allen Abteilungen der Behörde selbst, die berechtigt sind, die authentischen Daten einzusehen und für eigene Zwecke zu verwenden. Diese Berechtigung wird auf Basis der Empfehlung der Datenschutzbehörde gewährt.
Nutzerausschuss	Jede authentische Quelle muss über einen Nutzerausschuss verfügen. Der Nutzerausschuss handelt als übergreifendes Organ, das für das gute Funktionieren der Datenerfassung und des Datenaustausches verantwortlich ist. Er sorgt dafür, dass alle wichtigen Interessengruppen die Funktions- und Verfahrensweisen der authentischen Quelle mitbestimmen können. (Empfehlung 18/2012 der Ausschuss für den Schutz des Privatlebens, 23. Mai 2012) *Ausführliche Informationen über die Rollen für die Verwaltung einer authentischen Quelle finden Sie in Kapitel 2: „Wie erstelle ich eine authentische Quelle?“.*
Datenschutzbehörde	Die Datenschutzbehörde ist die belgische Behörde, die den Datenschutz bei der Verarbeitung personenbezogener Daten überwacht. Die Datenschutzbehörde ist seit dem Inkrafttreten der Datenschutz-Grundverordnung im Mai 2018 die Nachfolgerin der Ausschuss für den Schutz des Privatlebens.

	(Gesetz vom 3. Dezember 2017 zur Schaffung der Datenschutzbehörde, Artikel 2 und 4).
Dateninitiator	Der Dateninitiator ist die Organisation, die für die Erhebung, Eingabe, Validierung und Berichtigung von Daten verantwortlich ist. *Ausführliche Informationen über die Rollen für die Verwaltung einer authentischen Quelle finden Sie in Abschnitt 2.2.*
Datenschutz-Grundverordnung – General Data Protection Regulation (GDPR)	Die Datenschutz-Grundverordnung ist eine europäische Verordnung (Datum des Inkrafttretens: 25. Mai 2018), die mit den europäischen Datenschutzrechtsvorschriften harmonisiert wurde. Die Datenschutz-Grundverordnung bezweckt, personenbezogene Daten von Personen besser zu schützen. Dieses Gesetz hat zwei Anwendungsbereiche. Einerseits ist die Verordnung auf die Verarbeitung personenbezogener Daten durch europäische Unternehmen und Organisationen anwendbar, unabhängig vom Ort, an dem diese Verarbeitung erfolgt. Andererseits ist die Verordnung auf die Verarbeitung der personenbezogenen Daten von Bürgern der EU durch Unternehmen anwendbar, die nicht innerhalb der EU ansässig sind, wenn diese Unternehmen diesen Bürgern Güter, oder Dienstleistungen innerhalb der EU anbieten oder das Verhalten von EU-Bürgern überwachen, sofern dies innerhalb der EU erfolgt. (Datenschutz-Grundverordnung – General Data Protection Regulation, 25. Mai 2018)
Informationssicherheitsausschuss (ISA)	Der Informationssicherheitsausschuss ist ein unabhängiges Gremium, das bestimmt, welche personenbezogenen Daten geteilt werden dürfen und unter welchen Sicherheitsbedingungen dies zu erfolgen hat. Der ISA besteht aus einer Kammer für die soziale Sicherheit und Gesundheit und einer Kammer für die Föderalbehörde. (Gesetz vom 5. September 2018: *Loi instituant le comité de sécurité de l'information et modifiant diverses lois concernant la mise en oeuvre 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*).
Only-once-Gesetz	*„Das Gesetz vom 5. Mai 2014 zur Verankerung des Prinzips der einmaligen Datenerfassung in der Arbeitsweise der Dienste und Instanzen, die den öffentlichen Behörden unterstehen oder*

	bestimmte Aufträge für sie ausführen, und zur Vereinfachung und Harmonisierung von elektronischen Formularen und Papierformularen" ist allgemein als das Only-once-Gesetz bekannt. Aufgrund dieses Gesetzes müssen Instanzen verfügbare Daten aus den sogenannten (authentischen) Quellen wiederverwenden, statt sie erneut bei Bürgern oder Unternehmen anzufordern. Diesbezüglich wird die Bedeutung eines korrekten Datenaustausches zwischen den verschiedenen Instanzen hervorgehoben.
Datenschutz Auditprotokoll	Ein Datenschutz Auditprotokoll ist ein Protokoll, das automatisch vom System erzeugt wird und Informationen über die Abfrage oder Änderung (Erstellung, Anpassung und Löschung) von Daten umfasst. Diese Informationen sorgen dafür, dass man für jedes System immer überprüfen kann, welche Art von Abfrage oder Änderung von Daten durchgeführt wurde. *Ausführliche Informationen über das Datenschutz Auditprotokoll und den Audit Trail finden Sie in Abschnitt 2.4*.
Datenschutz Audit Trail	Ein Datenschutz Audit Trail wird durch Gruppierung der Auditprotokolle der verschiedenen Kettenpartner gebildet. Dieser Audit Trail sorgt dafür, dass die Transaktionen, die über den Dienste-Integrator durchgeführt werden, rekonstruiert werden können, sodass die gesetzliche Verpflichtung in Bezug auf personenbezogene Daten eingehalten werden kann *(Gesetz vom 8. Dezember 1992 über den Schutz des Privatlebens hinsichtlich der Verarbeitung personenbezogener Daten, Artikel 16).* *Ausführliche Informationen über das Datenschutz Auditprotokoll und den Audit Trail finden Sie in Abschnitt 2.4*.
Dienstleistungsvereinbarung	Eine Dienstleistungsvereinbarung (SLA) ist eine Vereinbarung, die abgeschlossen wird, um den Informationsaustausch zwischen den beiden beteiligten Parteien zu koordinieren. Eine Dienstleistungsvereinbarung umfasst einige Bedingungen und Komponenten, an die sich beide Parteien halten. *Ausführliche Informationen über Dienstleistungsvereinbarungen finden Sie in Abschnitt 2.5.*
Technischer Verwalter	Der technische Verwalter der (authentischen) Daten ist die Instanz, die für die Erarbeitung der technischen Modalitäten im Zusammenhang mit der Erfassung, Speicherung und Wartung der Daten und die Übermittlung von Daten an ihren Dienste-Integrator verantwortlich ist. Die Verbindung mit anderen

	Integratoren oder Instanzen wird vom gekoppelten Dienste-Integrator gesteuert. *Ausführliche Informationen über die Rollen für die Verwaltung einer authentischen Quelle finden Sie in Abschnitt 2.*
Sicherheitsberater	Ein Sicherheitsberater erteilt Ratschläge über alle Informationssicherheitsaspekte und sorgt für die betreffende Betreuung. Ein Sicherheitsberater wird als Experte für die Datenverarbeitung im Hinblick auf die Sicherheit der personenbezogenen Daten bestellt.