Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement des Innern EDI

Bundesamt für Statistik BFS
Abteilung Gesundheit und Soziales

Marco D'Angelo, 05.03.2020

Verknüpfungsrichtlinien

Version:	Datum:	Zweck:
0.1	22.05.2015	Arbeitsgruppensitzung vom 22.05.2015 (Titel „Aussprachepapier“)
0.2	08.06.2015	Arbeitsgruppensitzung vom 10.06.2015 (Titel „Aussprachepapier“)
0.3	17.06.2015	Arbeitsgruppensitzung vom 23.06.2015 (Titel „Aussprachepapier“)
0.9	24.06.2015	GL-Sitzung vom 01.07.2015 (Titel „Aussprachepapier“)
0.91	22.09.2015	Erster Entwurf für Arbeitsgruppensitzung vom 24.09.2015
0.93	24.09.2015	Entwurf für Arbeitsgruppensitzung vom 24.09.2015
0.94	29.09.2015	GL-Sitzung vom 07.10.2015
0.95	29.09.2015	GL-Sitzung vom 07.10.2015 (Version mit Änderungen)
0.96	27.10.2015	Version für Arbeitsgruppensitzung vom 19.11.2015
0.97	19.11.2015	Version für das BFS-Kolloquium vom 25.11.2015
1.1	08.11.2016	Version für Arbeitsgruppensitzung vom 20.12.2016 (Freigabe)
1.2	05.03.2020	Version mit Anpassungen an neue Rahmenbedingungen

Verteiler: GL, Arbeitsgruppe Verknüpfungen

Glossar

Abkürzung	Bedeutung
AC	Abteilungschef/in des BFS
BFS	Bundesamt für Statistik
BIT	Bundesamt für Informatik und Telekommunikation
BUR	Betriebs- und Unternehmensregister
BstatG	Bundesstatistikgesetz
COP	Code of Practice
EDI	Eidgenössisches Departement des innerns
FACH	Fachsektion des BFS
KD	Konsolidierte Daten
EDÖB	Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter
ETL	Extract, Transform, Load (Process)
GL	Geschäftsleitung des BFS
GWR	Gebäude- und Wohnungsregister
ISDS	Informationssicherheit und Datenschutz
IT	Sektion Informatik des BFS
METH	Sektion Statistische Methoden des BFS
MJP	Mehrjahresprogramm des BFS
OSS	On Site Support (des BIT)
RD	Rechtsdienst des BFS
RHG	Bundesgesetz über die Harmonisierung der Einwohnerregister und anderer amtlicher Personenregister
SAKE	Schweizerische Arbeitskräfteerhebung
SC	Sektionschef des BFS
SE	Strukturerhebung
SESAM	Syntheseerhebung Soziale Sicherheit und Arbeitsmarkt
SHIVALV	Sozialhilfe, Invalidenversicherung und Arbeitslosenversicherung
SHS	Sozialhilfestatistik
SILC	Erhebung über die Einkommen und Lebensbedingungen
SIS	Statistical Information System
SMS	Statistical Metadata System
SUS	Strafurteilsstatistik
STATENT	Statistik der Unternehmensstruktur
STATPOP	Statistik der Bevölkerung und der Haushalte
VDSG	Verordnung zum Bundesgesetz über den Datenschutz
VS	Verknüpfungsstelle des BFS

Inhaltsverzeichnis

1 Zusammenfassung

Datenverknüpfungen haben zum Ziel, Informationen aus bestehenden Daten zu gewinnen und dadurch Doppelspurigkeiten zu vermeiden, die Befragten zu entlasten, Synergien zu erzielen und erweiterte Informationsquellen zu erstellen. Eine Verknüpfung liegt dann vor, wenn zur Erfüllung der statistischen Aufgaben Einzeldaten aus verschiedenen Quellen miteinander verbunden werden und daraus ein neuer Datensatz entsteht. Dabei werden vier Verknüpfungsarten unterschieden, nämlich (i) systematische Verknüpfungen für die Statistikproduktion, (ii) Längsschnittverknüpfungen, (iii) Verknüpfungen für die Analyse und (iv) Spezialfälle. Die Verknüpfungen werden in einem Inventar erfasst (Nachvollziehbarkeit).
Verknüpfungsvorhaben im BFS unterliegen strengen Auflagen hinsichtlich Datenschutz und Datensicherheit. Alle Verknüpfungen müssen vom Direktor im Rahmen eines Antragsprozesses genehmigt werden. Innerhalb des BFS werden Sektoren definiert. Diese entsprechen den statistischen Produktionseinheiten und verfolgen das Ziel, konsolidierte Daten zu erstellen. Ausschliesslich autorisierte Mitarbeiter haben Zugriff auf diese Sektordaten (konsolidierte Daten). Die Datenverknüpfungen kann nur vornehmen, wer über die dazu erforderlichen Schlüssel zur De-Pseudonymisierung verfügt. Die Benutzung des Schlüssels setzt die Genehmigung der Verknüpfung voraus und wird protokolliert. Wenn der verknüpfte Datensatz die Schutzstufe 3 aufweist, muss ein Bearbeitungsreglement vorgelegt werden.
Zur Unterstützung der Verknüpfungsvorhaben werden zwei Gremien eingesetzt, nämlich die Verknüpfungsstelle, die die administrativen Arbeiten koordiniert und den Schlüsselschrank verwaltet, und die Arbeitsgruppe Verknüpfungen.
Die Anträge für Verknüpfungen können von BFS-internen oder BFS-externen Stellen eingereicht werden. Verknüpfungen werden primär vom BFS vorgenommen, unter Erfüllung bestimmter Voraussetzungen können auch Kantone und Gemeinden sowie Externe Daten des BFS verknüpfen.

2 Ausgangslage

Gemäss den initiierten Arbeiten zur Verknüpfungsthematik aus dem Jahr 2010[1] wurden die Arbeiten für ein Verknüpfungskonzept in drei Teile strukturiert.

- Allgemeine Ausrichtung
- Rechtsgrundlagen
- Organisation/Prozesse/Informatik

2014 wurde ein Bearbeitungsreglement vorgelegt (Bearbeitungsreglement „Verknüpfungen“. Stand vom 13. Oktober 2014). Dieses wurde dem Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) zur Beurteilung zugestellt, sein Feedback war positiv. Allerdings waren noch weitere Arbeiten erforderlich. In der Sitzung vom April 2015 wurde der Geschäftsleitung (GL) der Stand der Arbeiten präsentiert; auf dieser Grundlage hat die GL eine Auslegeordnung und Fragestellungen formuliert. Im Juli 2015 wurde in der GL ein Aussprachepapier vorgestellt und diskutiert, das auf dem Bearbeitungsreglement von 2014 basiert. Dieses wurde in die vorliegenden Verknüpfungsrichtlinien umgearbeitet und im Dezember 2015 von der GL verabschiedet.

2018 wurde dem EDÖB im Rahmen eines Besuchs im BFS die Vorgehensweise im Bereich der Datenverknüpfungen erläutert. Der EDÖB hat von der vom BFS erstellten Dokumentation Kenntnis genommen.

Auch den Gremien Fedestat und Korstat wurde im Rahmen von Besuchen am BFS die Botschaft übermittelt, dass Verknüpfungen im öffentlichen Statistiksystem der Schweiz eingebunden sind.

[1] Aussprachepapier 2010, Version 1.0 vom 25.8.2010

3 Ziele der Richtlinien

3.1 Vom erhebungsorientierten zum outputorientierten Ansatz

In der Vergangenheit waren die meisten Statistiken "erhebungsorientiert" konzipiert, d.h. für eine bestimmte Statistik wurde gezielt eine Erhebung durchgeführt. Um Doppelspurigkeiten zu vermeiden, die Befragten zu entlasten und vermehrt Synergien zu erzielen, findet in der Statistikproduktion eine effizienzsteigernde Weiterentwicklung statt. In Anwendung von Art. 4 BStatG sind statistische Daten in erster Linie ohne Durchführung von Direkterhebungen, d.h. durch konsequente Nutzung bestehender Register und Administrativdaten beizubringen. Im Sinne von outputorientierten, integrierten Informationssystemen wird die Datenerhebung entsprechend aus verschiedenen Quellen wie z.B. Register, Administrativdaten oder Befragungen koordiniert durchgeführt. Die Daten werden zur Erzeugung des gewünschten Outputs (Statistiken) zusammengeführt (verknüpft) und ausgewertet. Neben der verbesserten (Mehrfach-) Nutzung der erfassten Daten hat ein solches System den zusätzlichen Nutzen, dass neue Statistiken auf bereits vorhandenen Daten aufbauen können. Damit können die zunehmenden Informationsbedürfnisse der Nutzer aus Wirtschaft, Gesellschaft, Politik, Verwaltung oder Forschung besser abgedeckt werden.

3.2 Gewährleistung von Datenschutz und Datensicherheit

Das Statistikgesetz, das Datenschutzgesetz, der COP (Code of Practice von Eurostat), die Charta der öffentlichen Statistik und die Weisungen über die Informatiksicherheit in der Bundesverwaltung gelten auf Ebene des Amtes. Heute werden im BFS verschiedene Massnahmen angewendet, um Datenschutz und Datensicherheit zu gewährleisten:

- Zugriff über starke Authentifizierung (Winlogon mit Smartcard)
- Der Datenzugriff ist eingeschränkt auf die berechtigten Personen (Zugriffsregelung)
- Unterschriebenes Einverständnis mit den Datenschutzvorschriften von jedem Mitarbeitenden
- Anonymisierte Weitergabe von Einzeldaten
- Datenschutzverträge mit externen Nutzern

Für die Verknüpfungen müssen nun weitere Massnahmen ergriffen werden, insbesondere hinsichtlich Transparenz der Verknüpfungstätigkeit und der Prozesse sowie hinsichtlich Datenschutz und Pseudonymisierung von Einzeldaten.
Um den Anforderungen zu entsprechen und sicherzustellen, dass Datenverknüpfungen kontrolliert, gesichert und transparent durchgeführt werden, sind die folgenden Bereiche der Verknüpfungsaktivitäten im BFS zu regeln:

- die Begrifflichkeiten (Kap. 6.1)
- die massgeblichen Grundsätze (Kap. 6.2)
- die Voraussetzungen und Bedingungen für die Verknüpfung (Kap. 6.3)
- die technischen Vorkehrungen und der Umgang mit Daten (Kap. 7)
- die Organisation, Rollen und Verantwortlichkeiten (Kap. 8)
- die Verknüpfungsprozesse (Kap. 10).

4 Bezug zum statistischen Mehrjahresprogramm / Ziele (Amts-, Abteilungs- und Sektionsziele)

Gemäss dem Mehrjahresprogramm MJP 2015 – 2019 wird unter dem strategischen Ziel 3 „Die Bundesstatistik nutzt die geschaffenen Potenziale und passt die Diffusion ihrer statistischen Informationen den sich wandelnden Nutzerbedürfnissen an“ ein Schwerpunkt zur Datenverknüpfung aufgeführt. Dieser Schwerpunkt wird seitdem im MJP geführt

Im Rahmen der BFS Amtsziele ist das Ziel aus dem Mehrjahresprogramm berücksichtigt. Die Arbeitsgruppe Verknüpfungen erfüllt folgende Zielsetzung: „Das Potenzial der Datenverknüpfung wird gemäss definiertem Prozess und festgelegten Strukturen aktiv genutzt und durch Best Practices und abteilungsübergreifendem Austausch gefördert und laufend optimiert“.

5 Rechtlicher Rahmen

Die geltenden gesetzlichen Grundlagen, namentlich Art. 14*a* BStatG, Art. 16 Abs. 4 RHG, Art. 21 VDSG, Art. 13*h* ff Statistikerhebungsverordnung, die Datenverknüpfungsverordnung des EDI und die vorliegenden BFS- "Verknüpfungsrichtlinien", legen folgende rechtliche Rahmenbedingungen fest:

"Raison d'être": Der Aufwand für Befragte bei Direkterhebungen ist unter Umständen gross, was zu Unmut und Unverständnis gegenüber dem Bund (insbesondere BFS) führt bzw. die Rücklaufquoten negativ beeinflusst und zu qualitativ schlechteren Statistiken führt. Art. 4 Abs. 3 BStatG schreibt deshalb vor, dass die Zahl von Direkterhebungen auf ein notwendiges Minimum zu beschränken ist. Um trotzdem qualitativ hochstehende und repräsentative Statistiken erstellen zu können, soll das BFS die Möglichkeit der Datenverknüpfungen nutzen können.

Kompetenz: Auf Bundesebene hat ausschliesslich das BFS die Ermächtigung, Verknüpfungen zur Erfüllung seiner statistischen Aufgaben vorzunehmen. Es handelt sich um eine allgemeine Ermächtigung (Art. 14*a* BStatG). Art. 16 Abs. 4 RHG erlaubt zudem explizit die Verknüpfung von Daten aus den Einwohnerregistern mit Daten aus dem GWR und dem BUR.
Auf kantonaler und kommunaler Ebene dürfen Statistikstellen zur Erfüllung ihrer statistischen Aufgaben Daten des BFS verknüpfen, wenn sie dazu die schriftliche Zustimmung des BFS haben und dessen Auflagen berücksichtigen.
Andere Dritte (Auftraggeber) können im Interesse der Kosten- und Arbeitseffizienz in den Verknüpfungsprozess einbezogen werden. Die Einzelheiten sind ggf. klar im Datenschutzvertrag zu regeln.

Transparenz: *Jede* Datenverknüpfung setzt ein schriftliches und begründetes Gesuch voraus. Dieses muss von den betroffenen Fachsektionen, von der Sektion Statistische Methoden und vom Rechtsdienst auf seine fachliche, methodische und rechtliche Durchführbarkeit überprüft werden. Statistiken, für die systematisch Datenverknüpfungen durchgeführt werden, müssen im Anhang zur Statistikerhebungsverordnung als solche gekennzeichnet sein.

Datenschutz: Datenverknüpfungen dürfen nur durchgeführt werden, wenn sie für die statistischen Arbeiten geeignet und notwendig sind und die dazu erforderliche Qualität aufweisen. Eine Ausnahme bilden interne Spezialfälle bei denen spezifische Kriterien oder die Qualität der Daten getestet werden.
Die zur Durchführung von Datenverknüpfungen erforderlichen Schlüssel müssen zentral und in besonders gesicherter Form durch die Verknüpfungsstelle und nach dem Prinzip des Schlüssel-Managements aufbewahrt werden. Die dazu verwendeten Informatikmittel und Prozesse werden zentral zur Verfügung gestellt und sind für die Erstellung der Verknüpfungen verbindlich. Die Abgabe bzw. Benutzung eines Schlüssels im Einzelfall setzt die schriftliche Erlaubnis der Direktion voraus und muss protokolliert werden.
Die Zugriffsrechte auf die unterschiedlichen Daten (Input-, konsolidierte- und Produktdaten; siehe Kap. 7.1 und Anhang 1) müssen klar und restriktiv geregelt werden. Die unterschiedlichen Daten müssen separat verschlüsselt werden.

Für Datensammlungen (Erhebungen, Statistiken) mit Daten der Schutzstufe 3 müssen diese verschiedenen Sicherheitsmassnahmen in einem spezifischen Bearbeitungsreglement präzise definiert werden (Art. 21 Abs. 1 Bst. a VDSG). Ein Template für solche Erhebungen, das auf den Vorgaben des EDÖB basiert, liegt vor. Systematische Verknüpfungen im Rahmen von solchen Erhebungen und Statistiken müssen ebenfalls im Bearbeitungsreglement geregelt werden. Das Template enthält deshalb auch ein Kapitel "Verknüpfungen". Wenn für die Statistikproduktion bereits ein Bearbeitungsreglement vorliegt, wird dieses durch das Kapitel „Verknüpfungen“ ergänzt.
Das Erstellen eines spezifischen Bearbeitungsreglementes ist dagegen nicht grundsätzlich für jede einzelne Verknüpfung erforderlich. Werden Daten der Schutzstufe 3 verknüpft, ist die Verknüpfung unter Berücksichtigung der Bearbeitungsreglemente durchzuführen, die für diese Datenquellen bereits

(zwingend) vorhanden sind. Werden Daten der Schutzstufen 1-2 verknüpft, muss lediglich ein Bearbeitungsreglement erstellt werden, wenn die Output-Daten neu Schutzstufe 3 haben. Andernfalls reichen die vorliegenden Richtlinien in Verbindung mit den gesetzlichen Bestimmungen (namentlich Art. 13h ff Statistikerhebungsverordnung und Datenverknüpfungsverordnung des EDI) als Grundlagenregelung aus. Gemäss diesen Bestimmungen müssen aber alle Verknüpfungen ausführlich dokumentiert werden, dies insbesondere um dem Erfordernis der Transparenz Genüge leisten zu können. Entsprechende Informationen über Verknüpfungen sind in den Antragsformularen beziehungsweise im Entscheid des Direktors enthalten und sind im elektronischen Archiv des BFS abgelegt.

Verknüpfte Daten dürfen unter den Voraussetzungen von Art. 9 Statistikerhebungsverordnung weitergegeben werden, soweit das Gesetz die Datenweitergabe für nicht personenbezogene Zwecke wie Forschung, Planung und Statistik vorsieht. Sie ist abhängig von der Sensibilität der Daten, vom Verwendungszweck und vom Datenempfänger. Das BFS hat keine Pflicht, Daten weiterzugeben. Kantonale und kommunale Statistikstellen müssen den Datenschutz und die statistische Geheimhaltung in gleichem Masse garantieren wie das BFS; andernfalls kann das BFS einer Datenverknüpfung durch Letztere nicht zustimmen.

Die relevanten Gesetzestexte sind im Anhang 2 aufgeführt.

6 Verknüpfungsgrundlagen

6.1 Begrifflichkeiten

6.1.1 Was verstehen wir unter einer Verknüpfung?

Das BFS geht von der folgenden Verknüpfungsdefinition aus: Eine Verknüpfung liegt dann vor, wenn **Einzeldaten,** aus **verschiedenen Quellen** miteinander verbunden werden (Art. 13*h* Statistikerhebungsverordnung) und daraus ein **neuer Datensatz** entsteht. Gleiche Register oder Erhebungen, die zu unterschiedlichen Zeitpunkten ausgewertet bzw. durchgeführt werden, gelten dabei als unterschiedliche Datenquellen.[2] Damit es sich um eine Verknüpfung im Sinne der öffentlichen Statistik handelt, muss **mindestens eine der Datenquellen im Rahmen des BStatG** erarbeitet worden sein und die Verknüpfung der **Erfüllung von statistischen Aufgaben** dienen (gemäss Art. 14*a* des BStatG). Dabei werden die folgenden Verknüpfungskategorien unterschieden (siehe auch Kap. 6.1.2 Verknüpfungskategorien)

- Systematische Verknüpfungen für die Statistikproduktion
- Längsschnittverknüpfungen
- Verknüpfungen für die Statistikanalyse
- Spezialfälle

In den folgenden Fällen liegt keine Verknüpfung vor:

- Zeitreihen von aggregierten Einheiten (z.B. Preisindizes, Produktions- und Beschäftigungsentwicklung, Arbeitskräfteerhebung etc.). Es handelt sich hier nicht um Einzeldaten (siehe auch 6.1.2 → 2. auf S. 9)
- Die Verbindung von Daten mit Nomenklaturen oder das Hinzufügen von Geokoordinaten anhand von Adressinformationen. Dies dient lediglich der Bezeichnung oder Strukturierung bereits vorhandener Informationen.
- Die Zusammenführung von Daten aus verschiedenen Quellen im Betriebs- und Unternehmensregister (BUR) und im eidgenössischen Gebäude- und Wohnungsregister (GWR), soweit diese für die Registerführung und Registernutzung in den entsprechenden Verordnungen geregelt ist. Eine über diese Aktivitäten hinausgehende Verbindung von Daten unterliegt den Verknüpfungsvorschriften gemäss Erhebungsverordnung, Verknüpfungsverordnung des EDI und des zugehörigen Bearbeitungsreglements.

[2] Beispiele sind die Längsschnittverknüpfungen.

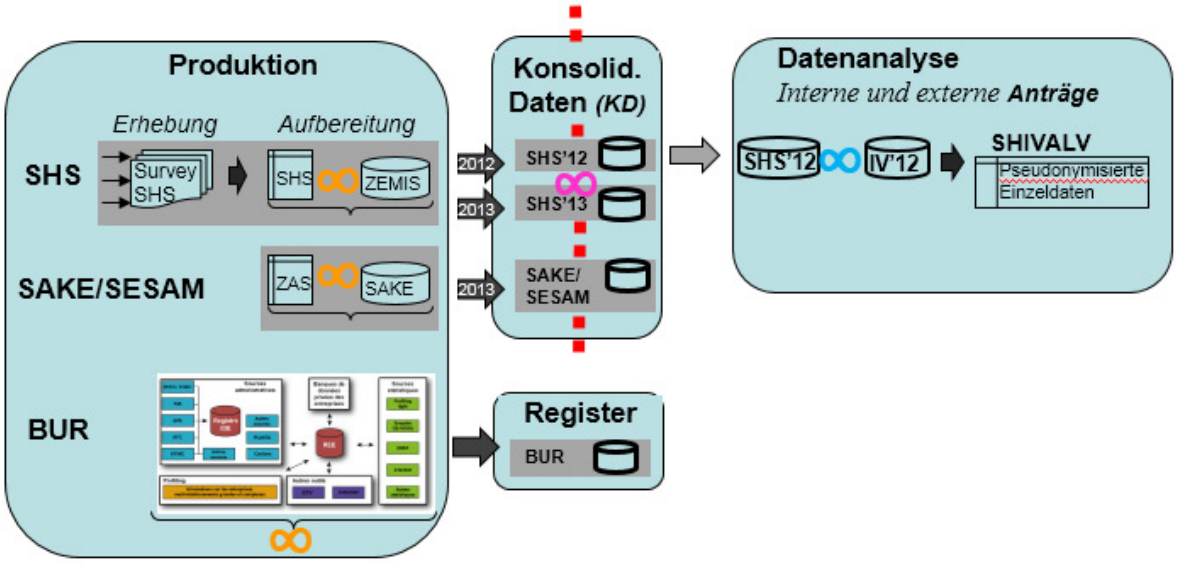
- Panelerhebungen, in welchen die Befragten die gleichen Fragen zu unterschiedlichen Zeitpunkten beantworten. Die Wiederverwendung von Personenbezeichnungen und Antworten aus den vorausgehenden Interviews ist bereits im Design der Erhebung vorgesehen und in der Statistikerhebungsverordnung aufgeführt. Es handelt sich hier um eine einzige Quelle und nicht um unterschiedliche Datenquellen.[3]
- Vergleich mit Vorjahresdaten aus der gleichen Erhebung im Prozess der Statistikproduktion zur Plausibilisierung und zur Qualitätskontrolle. Methodisch anspruchsvolle Verknüpfungsvorhaben im Sinne von technischen Machbarkeitstests gelten hingegen als Verknüpfungen und müssen ebenfalls inventarisiert sein (Spezialfälle).

6.1.2 Verknüpfungskategorien

Um eine hohe Akzeptanz und ein gemeinsames Verständnis zu erreichen, orientiert sich die Struktur der Verknüpfungen an einem Konzept, welches im BFS bereits eingeführt und bei den Mitarbeitenden und den Statistik-Fachleuten bestens bekannt ist, nämlich dem *Wertschöpfungsprozess für die Statistikproduktion* im BFS (siehe auch Kap. 7.1). Für jede Verknüpfung sind ein ausreichender Zweck und die rechtliche Basis eine notwendige Voraussetzung. Die meisten statistischen Aktivitäten sind in der *Statistikerhebungsverordnung* enthalten.

Aus vorgängigen Überlegungen ergeben sich vier Kategorien, welche Verknüpfungen charakterisieren:

1. Systematische Verknüpfungen für die Statistikproduktion
2. Längsschnittverknüpfungen
3. Verknüpfungen für die Statistikanalyse
4. Spezialfälle (in der Grafik nicht aufgeführt)



1. Systematische Verknüpfungen für die Statistikproduktion:
Systematische[4] Verknüpfungen für die Statistikproduktion zum Ziel der Erstellung von konsolidierten Daten (Input-Verknüpfungen) sind in der Statistikerhebungsverordnung aufgeführt (Bsp. SHS). Damit ist für alle diese Verknüpfungen die rechtliche Basis gegeben und gleichzeitig der Transparenz Folge geleistet. Unerheblich ist die Frage, ob vorgängig für die Erstellung von konsolidierten Daten eine Datenerhebung (Primärdaten) im BFS durchgeführt wird oder nicht. Als Produktion können auch Verknüpfungen von zwei Datenquellen in der Statistikerhebungsverordnung aufgeführt sein (Bsp.

[3] Hingegen gelten beispielsweise bei der SAKE und bei SILC die Verknüpfung mit Daten aus STATPOP und dem BUR als Verknüpfung im Sinne dieser Richtlinien.
[4] Im Sinne von wiederkehrend

SAKE/SESAM).
Vergleiche mit Datenquellen einzig für die Qualitätssicherung oder Datenaufbereitung im Rahmen der Produktion von konsolidierten Daten sind in der Statistikerhebungsverordnung nicht aufzuführen.

Anreicherungen/Datenzusammenführungen in Verzeichnissen und Registern
Ein besonderer Prozess bei der Statistikproduktion ist die Verknüpfung respektive die Anreicherung von Registern und Verzeichnissen mit Daten. Man spricht hier auch von administrativen Datenquellen. Diese Zusammenführung von Daten ist ebenfalls als eine Verknüpfung zu betrachten und kann ebenfalls in der Statistikerhebungsverordnung stehen (Bsp. BUR, STATENT, GWR, etc.). Speziell bei diesen Verknüpfungen ist, dass sie teilweise eine eigene gesetzliche Basis haben und sich als Register nicht am „klassischen" Wertschöpfungsprozess für Statistikproduktionen orientieren.

Merkmale von systematischen Verknüpfungen für die Statistikproduktion

- Nur BFS-intern
- Produktionscharakter
- Aufgeführt in der Statistikerhebungsverordnung (als Erhebung oder Statistik)
- Einmaliges Bewilligungsverfahren notwendig. Wenn danach die Verknüpfung im Anhang aufgeführt ist, erfolgt die Bewilligung im Rahmen der jährlichen Anpassung der Statistikerhebungsverordnung

Anreicherungen/Datenzusammenführungen in Verzeichnissen und Registern

- „Eigene" Registerverordnung
- Quellen, die mit dem Register/Verzeichnis zusammengeführt werden, sind transparent ausgewiesen

2. Längsschnittverknüpfungen

Als Längsschnittverknüpfung wird das Zusammenfügen von Variablen derselben Einheiten aus Erhebungen oder administrativen Datenquellen zu unterschiedlichen Zeitpunkten (z.B. jährliche oder mehrjährige Erhebungen) zur Erlangung von Informationen über Veränderungen oder Verläufe verstanden. Verknüpfungen beziehen sich nur auf Einzeldaten, Zeitreihen von aggregierten Einheiten sind im Kontext der Verknüpfung nicht betroffen (z.B. Preisindizes, Produktions- und Beschäftigungsentwicklung, Erwerbslosenquote etc.).

Positive Beispiele für Längsschnittverknüpfungen:
1) Die Verbindung von Einzeldaten aus Erhebungen unterschiedlicher Zeitpunkte (z.B. Unternehmensdemografie) zwecks Darstellung von Veränderungen oder Entwicklungen im Zeitablauf.
2) Die Erstellung von individuellen Bildungsverläufen durch Zusammenführen von Informationen aus Erhebungen, die sich auf unterschiedliche Zeitpunkte oder Perioden beziehen.

Negative Beispiele für Längsschnittverknüpfungen:
1) Vergleich mit Einzeldaten aus dem Vorjahr zur Kontrolle der Angaben und zur Qualitätskontrolle (z.B. Wertschöpfungsstatistik, Pensionskassenstatistik).
2) Panelerhebungen, wie SILC oder SAKE, in welcher die Befragten die gleichen Fragen zu unterschiedlichen Zeitpunkten beantworten. Die Wiederverwendung von Personenbezeichnungen und Antworten aus den vorausgehenden Interviews ist bereits im Design der Erhebung vorgesehen und in der Statistikerhebungsverordnung aufgeführt.

Längsschnittverknüpfungen werden BFS-intern und durch das BFS vorgenommen. Im Regelfall werden die konsolidierten Daten einer Erhebung über mehrere Zeiteinheiten verknüpft. Diese Verknüpfung kann als „Produkt" angesehen werden, welches das BFS inventarisiert. Falls externe Nutzer solche konsolidierten Daten über mehrere Zeiteinheiten verwenden wollen, kann dies über einen üblichen Datenschutzvertrag abgewickelt werden. Dasselbe gilt auch, wenn die Datenlieferung nicht alle Variablen des Gesamtprodukts umfasst.

Merkmale von Längsschnittverknüpfungen

- Mehrheitlich BFS-intern (Längsschnittverknüpfungen, die speziell für Externe erstellt werden, sind grundsätzlich auch möglich, dann kommt aber der Bearbeitungsprozess „Verknüpfungen für Statistikanalysen“ für Externe zum Tragen)
- Zweck der Datenverknüpfung ist primär die Analyse
- Tendenziell standardisierte „Produkte“
- Laufendes Bewilligungsverfahren für BFS-interne Verknüpfungen (Ergänzung im Bearbeitungsreglement der Erhebung oder Produktion)
- Aufnahme im BFS-Inventar „Längsschnittverknüpfungen“
- Bei systematischer Verknüpfung ist die Aufnahme in die Statistikerhebungsverordnung gemäss Art. 13*n* Statistikerhebungsverordnung notwendig

Externe können bereits bestehende Längsschnittverknüpfungen über den Prozess von Datenschutzverträgen erhalten.

3. Verknüpfungen für Statistikanalysen

Statistische Verknüpfungen (Output-Verknüpfungen), die das BFS gestützt auf Art. 14a BStatG zur Erfüllung seiner statistischen Aufgaben vornehmen kann, müssen zur Sicherstellung der rechtlichen Anforderungen und aus Transparenzgründen über dokumentierte Anträge erfolgen. Dies gilt für BFS-interne wie externe Anträge. Diese Verknüpfungen dienen nicht der Produktion, sondern der statistischen Analyse (z.B. Bildungsverläufe, Projekt NCCR der Universität Genf)

Merkmale von Verknüpfungen für Statistikanalysen

- Verwendung der verknüpften Daten BFS-intern oder für externe Antragsteller
- Analyse-Charakter
- Mehrheitlich einmalig
- Anträge gemäss Prozess in diesem Dokument (siehe Kap 10 und Anhang 5)
- Aufnahme im BFS-Inventar „Verknüpfungen für Analyse“.

4. Spezialfälle

Alle übrigen Verknüpfungen, die nicht einer der drei vorgenannten Verknüpfungen angehören, werden ebenfalls transparent ausgewiesen und sind in der Kategorie der Spezialfälle zusammengefasst. Dabei gilt als Faustregel: Methodisch anspruchsvolle Verknüpfungsvorhaben im Sinne von technischen Machbarkeitstests gelten als Spezialfälle von Verknüpfungen, Vergleiche mit Einzeldaten aus dem Vorjahr zur Kontrolle der Angaben und zur Qualitätskontrolle gelten nicht als Verknüpfungen.

Merkmale von Spezialfällen

- BFS-intern: Einmalig im Sinne von technischen Machbarkeitstests
- Antrag gemäss Prozess im Abschnitt 6.3 dieser Verknüpfungsrichtlinien
- Aufnahme im BFS-Inventar „Verknüpfungen Spezialfälle“

6.2 Massgebliche Grundsätze

Die Erfahrungen haben bestätigt, dass es einen integralen Ansatz braucht und die Verknüpfungsdefinition weit gefasst werden muss. Das Ziel ist darum, allgemeine Grundsätze festzulegen, die für das ganze BFS gelten und in den operativen Einheiten fachspezifisch umgesetzt werden.

Bei der Verknüpfung von Daten orientiert sich das BFS an den nachfolgend aufgeführten Grundsätzen:

- Die Verknüpfung von Daten zur effizienten und Ressourcen schonenden Gewinnung von statistischen Informationen ist ein vom BFS unterstütztes und gezielt eingesetztes Vorgehen.
- Verknüpfungen werden nur zu statistischen Zwecken im Sinne des Bundestatistikgesetzes vorgenommen; sie müssen notwendig und verhältnismässig sein. Der Informationsbedarf muss nachgewiesen sein; es gibt keine Verknüpfungen auf Vorrat.
- Die Verknüpfungen im BFS sind transparent aufgeführt und dokumentiert. Die rechtliche Basis ist geprüft, die Verknüpfungen sind inventarisiert und von der Direktion des BFS freigegeben.
- Verknüpfungen müssen statistisch-methodisch korrekt und vertretbar sein. Sowohl die Input- als auch die Output-Daten müssen den gängigen statistischen Qualitätsansprüchen genügen.
- Die Verknüpfungs-Prozesse erfüllen hohe Datenschutz- und Datensicherheitsansprüche. Sie werden mit den dafür vorgesehenen Hilfsmitteln ausgeführt und sind sowohl zentral kontrolliert als auch dokumentiert.
- Die Detailprozesse sind im konkreten Falle möglichst einfach und benutzerfreundlich auszugestalten. Unnötige Komplikationen und administrative Belastungen sind möglichst zu vermeiden.
- Die Prozessschritte, die in diesen Verknüpfungsrichtlinien dargestellt sind (siehe Kap. 6.3 Vorgaben für Verknüpfungen, Kap. 10 Verknüpfungsprozesse und Anhang 5: Prozessbeschreibungen), gelten für alle Antragsteller gleichermassen (interne und externe).
- Verknüpfungen gemäss Art. 14*a* BStatG werden hauptsächlich durch das BFS vorgenommen. Sind die nötigen Voraussetzungen erfüllt, ist auch eine Delegation gewisser Verknüpfungsaufgaben an Dritte möglich (siehe 10.3.2).
- Das BFS prüft die rechtlichen Voraussetzungen (z.B.: Sind Rechtsgrundlagen für das beantragte Vorhaben vorhanden? Entspricht das Vorhaben den rechtlichen Bestimmungen?) sowie die inhaltliche, methodische und technische Realisierbarkeit möglichst innerhalb von 15 Arbeitstagen nach Eintreffen des Antrags.
- Die Weitergabe von verknüpften Daten ist im Rahmen der Regelungen zur Weitergabe von Einzeldaten grundsätzlich möglich (Art. 13/ Statistikerhebungsverordnung). Sie ist abhängig von der Sensibilität der Daten, vom Verwendungszweck und vom Datenempfänger. In jedem Fall ist ein Datenschutzvertrag zu erstellen.
- Zusätzlich zu den im vorliegenden Dokument festgehaltenen Bestimmungen im Zusammenhang mit der Datenverknüpfung gelten die in anderen Regelwerken des BFS festgehaltenen Vorschriften zur Behandlung und Weitergabe von Einzeldaten sowie zum Datenschutz und zur Datensicherheit[5].
- Für die Verrechnung des Aufwandes zur Durchführung von Datenverknüpfungen ist die Verordnung über die Gebühren und Entschädigungen für statistische Dienstleistungen von Verwaltungseinheiten des Bundes massgeblich.

[5] Wegleitung zum Datenschutz bei der Weitergabe von Einzeldaten an Dritte, 18.10.2006

6.3 Vorgaben für Verknüpfungen

Verknüpfungskategorien und ihre Voraussetzungen: Intern

	Vorgaben für den Ablauf			
Verknüpfungskategorie	**Vorher**	**Ausführung (siehe auch Kap. 10.3.1)**	**Nachher**	**Vorbehalte/ Erleichterungen**
1) Systematische Verknüpfung für Statistikproduktion	• Antrag gemäss Formular (siehe Anhang 5) • Beurteilung Fach, METH und RD • Entscheid AC, Information der anderen GL-Mitglieder • Entscheid Direktion • Beantragung Erstellung Schlüssel durch Fachsektion an IT*. • Das Modul Verknüpfung im Bearbeitungsreglement ist nachgeführt (nur bei Schutzstufe 3) • Antrag/Anmeldung auf Aufnahme in den Anhang der Statistikerhebungsverordnung • Aufnahme ins Inventar	• Freigabe Schlüssel* an Sektorverantwortlichen • De-Pseudonymisierung (von Stufe 2 zu Stufe 1, siehe Kap 7.3) • Fallspezifische Pseudonymisierung/Verknüpfung	• Ende Gültigkeit Berechtigung zur Verwendung des Schlüssels	• Für bestehende Verknüpfungen, die bereits im Anhang der Statistikerh.V aufgeführt sind, muss kein Antrag gestellt werden. • Kein Löschen des verknüpften Datensatzes

Anreicherung/ Datenzusammenführungen in Verzeichnissen und Registern	• Dokumentation • Bearbeitungsreglement (nur bei Schutzstufe 3) • Spezielle gesetzliche Grundlage		• Schlussdokumentation	• Vereinfachung des Verfahrens bei nicht sensiblen Daten zulässig • Kein Löschen des verknüpften Datensatzes
2) Längsschnittverknüpfungen	• Antrag gemäss Formular (siehe Anhang 5) • Beurteilung Fach, METH und RD • Entscheid AC, Information der anderen GL-Mitglieder • Entscheid Direktion • Beantragung Erstellung Schlüssel durch Fachsektion an IT*. • Das Modul Verknüpfung im Bearbeitungsreglement ist nachgeführt (nur bei Schutzstufe 3) • Antrag/Anmeldung auf Aufnahme in den Anhang der Statistikerh.V • Aufnahme ins Inventar	• Freigabe Schlüssel* an Sektorverantwortlichen • De-Pseudonymisierung (von Stufe 2 zu Stufe 1, siehe Kap 7.3) • Fallspezifische Pseudonymisierung/Verknüpfung	• Ende Gültigkeit Berechtigung zur Verwendung des Schlüssels	• Vereinfachung des Verfahrens bei nicht sensiblen Daten zulässig • Kein Löschen des verknüpften Datensatzes • Zusätzliche Sicherheitsmassnahmen oder Einschränkungen bei Datenweitergabe/ -nutzung von sensiblen Daten
3) Verknüpfungen für die Statistikanalyse	• Antrag gemäss Formular (siehe Anhang 5) • Beurteilung Fach, METH und RD • Entscheid AC, Information der anderen GL-Mitglieder • Entscheid Direktion	• Freigabe Schlüssel* an Sektorverantwortlichen • De-Pseudonymisierung (von Stufe 2 zu Stufe 1, siehe Kap 7.3) • Fallspezifische Pseudonymisierung/Verknüpfung	• Ende Gültigkeit Berechtigung zur Verwendung des Schlüssels	• Vereinfachung des Verfahrens bei nicht sensiblen Daten zulässig • zusätzliche Sicherheitsmassnahmen oder Einschränkungen bei Datenweitergabe/ -nutzung bei sensiblen Daten

	• Beantragung Erstellung Schlüssel durch Fachsektion an IT*. • Erstellen eines spez. Bearbeitungsreglements, wenn Output-Daten neu Schutzstufe 3 • Aufnahme ins Inventar			• Löschen von sensiblen Datenverknüpfungen nach erfolgter Analyse
4) Spezialfälle (Testverknüpfungen) für interne Zwecke	• Antrag via Linie gemäss vereinfachtem Prozess (ohne RD/METH) • Beurteilung Fach • Entscheid AC, Information der anderen GL-Mitglieder • Entscheid Direktion • Beantragung Erstellung Schlüssel durch Fachsektion an IT*. • Das Modul Verknüpfung im Bearbeitungsreglement ist nachgeführt (nur bei Schutzstufe 3) • Aufnahme ins Inventar	• Freigabe Schlüssel* an Sektorverantwortlichen • De-Pseudonymisierung (von Stufe 2 zu Stufe 1, siehe Kap 7.3) • Fallspezifische Pseudonymisierung/Verknüpfung	• Ende Gültigkeit Berechtigung zur Verwendung des Schlüssels	• Aufnahme im BFS-Inventar • Zusätzliche Sicherheitsmassnahmen möglich bei der Verknüpfung von sensiblen Daten • Löschen von sensiblen Datenverknüpfungen nach Abschluss der Tests

Verknüpfungskategorien und ihre Voraussetzungen: Extern

	Voraussetzungen			
Verknüpfungskategorie	**Vorher**	**Ausführung**	**Nachher**	**Vorbehalte/ Erleichterungen**
1) Systematische Verknüpfung für Statistikproduktion	-	-	-	-

Anreicherung/ Datenzusammenführungen in Verzeichnissen und Registern	-	-	-	-
2) Längsschnittverknüpfungen	• Antrag gemäss Formular • Beurteilung Fach, METH und RD • Entscheid AC, Information der anderen GL-Mitglieder • Entscheid Direktion • Beantragung Erstellung Schlüssel durch Fachsektion an IT*. • Erstellen Datenschutz- und Verknüpfungsvertrages • Aufnahme ins Inventar	• Freigabe Schlüssel* an Sektorverantwortlichen • De-Pseudonymisierung (von Stufe 2 zu Stufe 1, siehe Kap 7.3) • Fallspezifische Pseudonymisierung/Verknüpfung • ggf. Prüfung der Output-Daten durch BFS	• Ende Gültigkeit Berechtigung zur Verwendung des Schlüssels- Datenweitergabe	• Vereinfachung des Verfahrens bei nicht sensiblen Daten zulässig • Zusätzliche Sicherheitsmassnahmen oder Einschränkungen bei Datenweitergabe/ -nutzung bei sensiblen Daten • Dritte werden ggf. bei Bedarf in die Verknüpfungsarbeiten involviert (siehe 10.3.2)
3) Verknüpfungen für die Statistikanalyse	• Antrag gem. Formular • Beurteilung Fach, METH und RD • Entscheid AC, Information der anderen GL-Mitglieder • Entscheid Direktion • Beantragung Erstellung Schlüssel durch Fachsektion an IT*. • Erstellen Datenschutz- und Verknüpfungsvertrag • Aufnahme ins Inventar	• Freigabe Schlüssel* an Sektorverantwortlicher • De-Pseudonymisierung (von Stufe 2 zu Stufe 1, siehe Kap 7.3) • Fallspezifische Pseudonymisierung/Verknüpfung • ggf. Prüfung der Output-Daten durch BFS	• Ende Gültigkeit Berechtigung zur Verwendung des Schlüssels- Datenweitergabe	• Vereinfachung des Verfahrens bei nicht sensiblen Daten zulässig • Zusätzliche Sicherheitsmassnahmen oder Einschränkungen bei Datenweitergabe /- nutzung von sensiblen Daten • Löschen von sensiblen Datenverknüpfungen nach erfolgter Analyse • Dritte werden ggf. bei Bedarf in die Verknüpfungsarbeiten involviert (siehe 10.3.2)

* Die Freigabe des Schlüssels erfolgt über den Entscheid der Direktion zur Durchführung einer Verknüpfung Die Sektion IT verwaltet aus technischer Sicht das Tool zur Erstellung und Verwendung der Schlüssel im Auftrag der Verknüpfungsstelle. Die Existenz einer GEVER-Referenznummer wird vorausgesetzt, da diese mit dem Direktionsentscheid zusammenhängt.

6.4 Datensensibilität

Im Zusammenhang mit Verknüpfungen spielt die Sensibilität der implizierten Daten eine wichtige Rolle. Dabei ist sowohl der Sensibilität der zu verknüpfenden Daten (Input-Daten) als auch der durch die Verknüpfung entstehenden Daten (Output-Daten) Aufmerksamkeit zu schenken. Je nach Sensibilität müssen mehr oder weniger strenge Massnahmen (beschränkte Weitergabe, Löschung etc.) ergriffen werden. Je sensibler die Daten sind, desto schutzwürdiger sind sie. Es werden vier Schutzstufen unterschieden:

Schutzstufen

(aus "Wegleitung zum Datenschutz bei der Weitergabe von Einzeldaten an Dritte", Stand 18.10.2006)

- ***Stufe 0 (Sachdaten)**:*
  Nicht personenbezogene Daten, z.B. Messdaten.

- ***Stufe 1 (einfache Personendaten)**:*
  Daten, die kein relevantes Gefährdungspotenzial für die Persönlichkeit der betroffenen natürlichen oder juristischen Personen beinhalten (z.B. Name, Vorname, Adresse, Geburtsdatum, Branchenzugehörigkeit eines Betriebes). Zusammen mit besonders schützenswerten Daten können solche Daten jedoch zu einer höheren Schutzstufe gehören, z.B. Namen der Insassen einer Strafanstalt oder einer Aids-Klinik. Daten der Stufe 1 sind zudem oft relativ leicht zugänglich (Telefonbuch, Jahresberichte, andere Veröffentlichungen) und können mit entsprechendem Aufwand auch von Dritten, unabhängig vom BFS, erhoben werden.

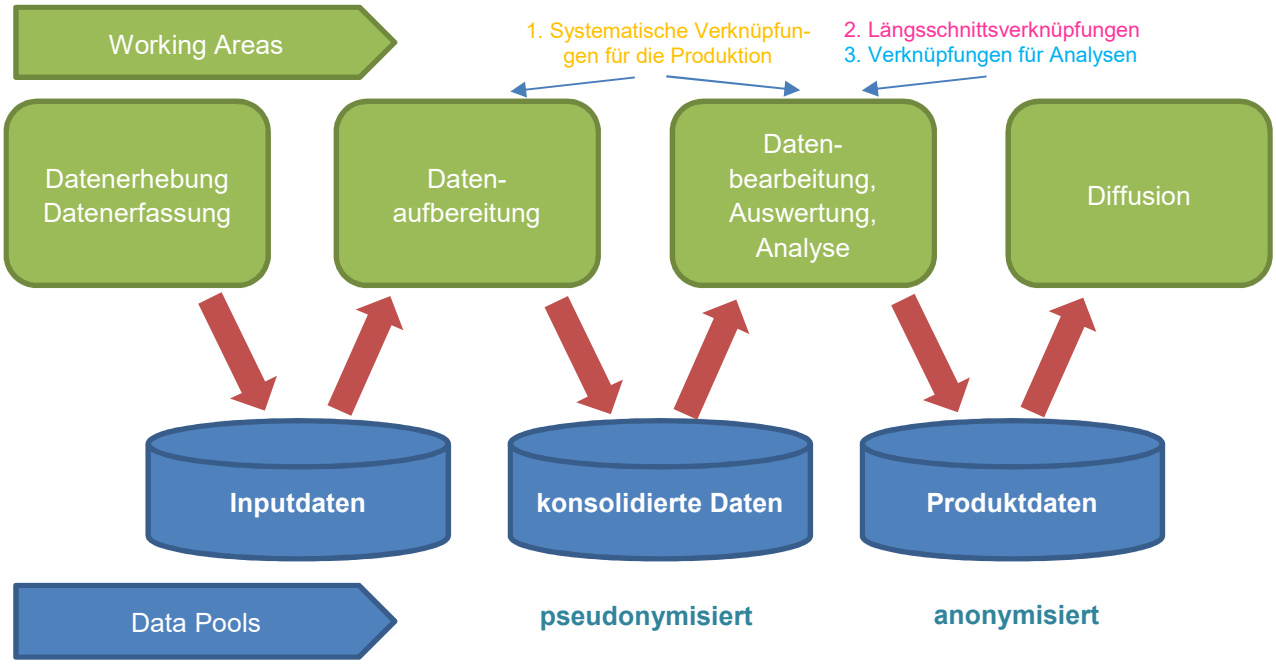
- ***Stufe 2 (qualifizierte Personendaten)**:*
  Daten, die ein gewisses Gefährdungspotenzial für die Persönlichkeit der betroffenen natürlichen oder juristischen Personen beinhalten (z.B. Einkommens- und Vermögensdaten, Mietpreise, Geschäftsbeziehungen, Daten über Bildung, Erwerb, Meinungen und Verhalten in den nicht zur Stufe 3 gehörenden Bereichen).

- ***Stufe 3 (besonders schützenswerte Personendaten)**:*
  Daten, die ein grosses Gefährdungspotenzial für die Persönlichkeit der betroffenen natürlichen oder juristischen Personen beinhalten (z.B. Angaben über Religion, weltanschauliche, gewerkschaftliche, politische Ansichten und Tätigkeiten, Rasse, Gesundheit, Intimsphäre, Sozialhilfe, Straftaten).

7 Statistikproduktion, Datensicherheit und Datenverknüpfung

7.1 Statistik-Produktionsprozess

In der Statistikproduktion wird generell nach den folgenden Prozessschritten unterschieden: ⇨Datenerhebung/Datenerfassung ⇨Datenaufbereitung ⇨Datenbearbeitung, Auswertung, Analyse ⇨ Diffusion.
Die meisten Statistikproduktionen funktionieren nach diesem Grundschema:



Die verschiedenen Prozessschritte umfassen im Einzelnen die folgenden Aktivitäten:

Datenerhebung, Datenerfassung

- Durchführen von Erhebungen *(Direkterhebungen, Register, Administrativdaten etc.)* und Befragungen, welche entsprechend dokumentiert sind durch Konzepte, Schnittstellenbeschreibungen der zu erhebenden Variablen usw. oder Übernahme von Daten aus administrativen Quellen, Registern, Messungen usw.
- Erfassen der Daten.
- Speichern der Inputdaten *(Inputdaten sind Rohdaten aus den Erhebungen. Sie enthalten in der Regel noch identifizierende (Personen-) Merkmale, die für die Aufbereitung und für allfällige Rückfragen bei den Datenlieferanten benötigt werden -> Siehe Anhang 1)*.

Datenaufbereitung

- Ausgehend von den Inputdaten wird die Datenaufbereitung durchgeführt, in welcher Inkonsistenzen, fehlende Werte und Ausreisser bearbeitet und zudem Synthesevariablen (abgeleitete Merkmale) berechnet werden. Dabei können auch Datenverknüpfungen vorgenommen werden. Datenverknüpfungen, die im Rahmen der Statistikproduktion systematisiert und in den entsprechenden Dokumentationen (Grob- und Detailkonzepte, Bearbeitungsreglemente für die Erhebung, ISDS etc.) vorgesehen sind, werden im Anhang der Erhebungsverordnung aufgeführt (Verknüpfungen für die Statistikproduktion).
- Die aufbereiteten Daten werden als „konsolidierte Daten“ gespeichert *(Konsolidierte Daten sind aufbereitete und bereinigte Einzeldaten. Sie werden in pseudonymisierter Form gehalten. Identifizierende Personenmerkmale (Namen, Adressen usw.) werden nicht übernommen und übergreifende Identifikatoren (wie AHV-Nr., UID usw.) werden pseudonymisiert -> Siehe Anhang 1)*. Im Sinne einer **Best Practice** gilt: Die konsolidierten Daten (KD) werden gemäss SIS-Konzept in der zentralen Datenbank KD abgelegt.

Der Zugriff für Verknüpfungen erfolgt ausschliesslich über gesicherte ETL Prozesse. Es gibt keinen direkten Datenzugriff.

Datenbearbeitung, Auswertung, Analyse

- Ausgehend von den konsolidierten Daten werden weitere Bearbeitungen vorgenommen, z.B. Auswertungen erstellt, Analysen durchgeführt oder Daten verknüpft (Längsschnittverknüpfungen oder Verknüpfungen für die Datenanalyse).
- Diese Weiterbearbeitung der Daten erfolgt grundsätzlich in pseudonymisierter Form.
- Ergebnisse dieser Weiterbearbeitung werden als „Produktdaten“ (*meistens in aggregierter und somit anonymisierter Form -> Siehe Anhang 1*) oder wieder als „konsolidierte Daten“ abgespeichert, sofern sie nicht gemäss Art. 14a BStatG aus Sensibilitätsgründen gelöscht werden müssen.

Diffusion

- Ausgehend von den Produktdaten werden Diffusions-Artikel erstellt und den interessierten Kunden in geeigneter Form zur Verfügung gestellt.
- Die konsolidierten Daten sind die Basis für die BFS-Produkte (Tabellen, Cubes, Datamarts für Datenlieferungsverträge, Kartographie, etc.).

7.2 Datenschutz

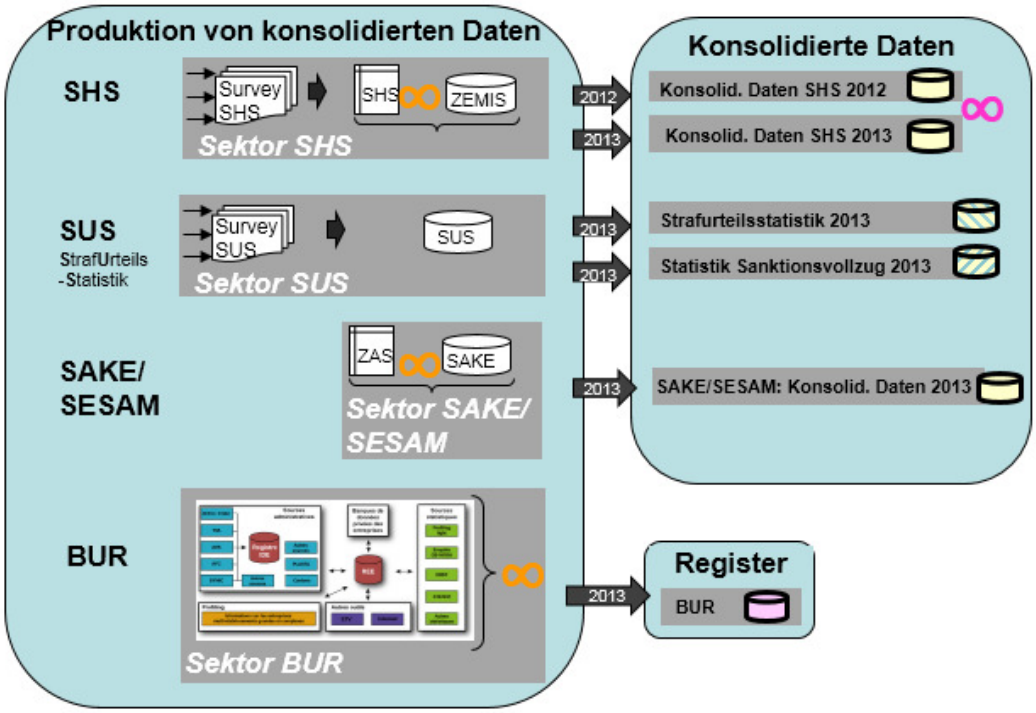
Das BFS garantiert Datenschutz und -sicherheit auch bei Verknüpfungen. Verknüpfungen stehen zunehmend im Fokus des öffentlichen Interesses. Darum muss das BFS seine Aktivitäten einfach und transparent beschreiben, um das ins BFS gesetzte Vertrauen weiterhin sicherzustellen.
Entsprechend kennen die Mitarbeitenden die Vorteile, aber auch die Gefahren von Datenverknüpfungen und können die BFS-Aktivitäten einfach gegen aussen kommunizieren. Anfragen von Ämtern oder dem EDÖB über die statistische Tätigkeit können transparent, umfassend und rasch beantwortet werden.
Das Statistik- und das Datenschutzgesetz, die Vorgaben des COP, die Charta der öffentlichen Statistik und die Weisungen über die Informatiksicherheit in der Bundesverwaltung sind für das BFS verbindlich. Entsprechend werden die Massnahmen umgesetzt wie bspw. die Unterzeichnung der Einhaltung der COP-Vorgaben durch jeden einzelnen Mitarbeitenden. Die Abteilungen legen die Sektoren fest, anschliessend definieren die Sektorverantwortlichen den Zugriff auf die Inputdaten resp. Datenquellen innerhalb des Sektors. Die Sektoren wiederum stellen die Pseudonymisierung der konsolidierten Daten sicher. Der Sektorenverantwortliche ist für deren Zugriff verantwortlich. Das Rollenkonzept in Kapitel 8 regelt die weiteren Details.
Es gibt drei Ebenen mit jeweils eigenen Massnahmen, um die verknüpften Daten vor unautorisiertem Zugriff zu schützen (zusätzlichen Schutz bieten die Pseudonymisierung und das Schlüsselmanagement):

7.2.1 Vertrauensraum BFS

Die Ebene des Vertrauensraumes BFS ist durch die relevanten Gesetze, die Charta der öffentlichen Statistik und den Code of Practice (COP) definiert. Diese Vorschriften gelten für alle BFS-Mitarbeitenden und stellen die erste Schutzstufe dar.

7.2.2 Sektoren

Die Ebene der Sektoren entspricht den statistischen Produktionseinheiten im BFS. Diese verfolgen das Ziel, konsolidierte Daten aus der Datenerhebung für die Datenbearbeitung, Auswertung und Analyse zu erstellen. In der nachfolgenden Grafik sind vier Sektoren beispielhaft aufgeführt: SHS, SUS, SAKE/SESAM und BUR.



Ein Sektor verfügt in der Regel über eine Erhebungsapplikation mit Inputdaten wie im Falle von SHS oder SUS. Aber auch Produktionseinheiten, welche keine Inputdaten erheben und aus verschiedenen Quellen ein Statistikprodukt (konsolidierte Daten) erstellen (z.B. SAKE/SESAM), können als Sektor gelten.
Die Sektoren schützen die Daten, indem der Zugriff auf die zu verarbeitenden Inputdaten eingeschränkt und kontrolliert wird. Nur Mitarbeitende der Produktionseinheit, welche für die Bearbeitung der Inputdaten autorisiert sind, erhalten einen Zugriff auf die Erhebungsapplikation (Beispiel SHS) respektive das Produktionsinstrument (Beispiel SAKE/SESAM), wenn keine Applikation für die Erhebung existiert.
Je feiner die Einteilung der Sektoren, desto eingeschränkter ist die Möglichkeit, Daten ohne weiteres miteinander zu verknüpfen.

7.2.3 Pseudonymisierung von konsolidierten Daten

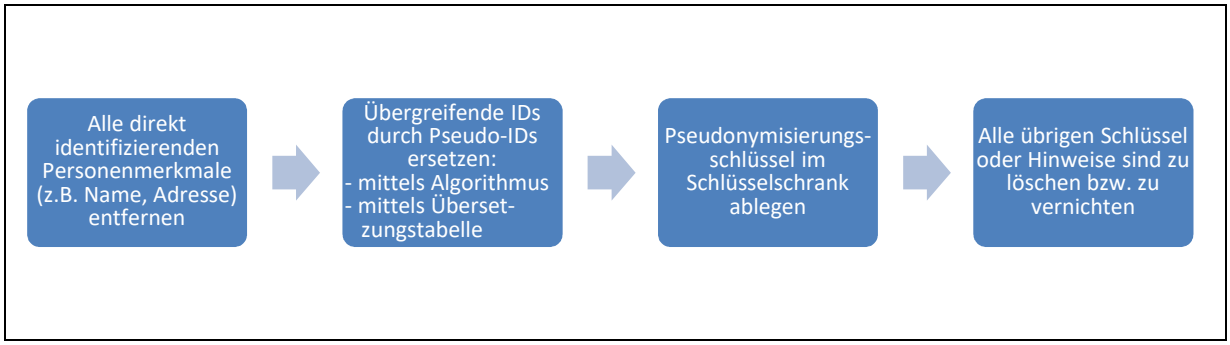
Durch die Pseudonymisierung der konsolidierten Daten (jede Erstellung von konsolidierten Daten hat eigene, mit anderen konsolidierten Daten nicht vergleichbare Pseudoidentifikatoren) können keine nicht-autorisierten Verknüpfungen von konsolidierten Einzeldaten vorgenommen werden. Die Vergabe und Verwaltung der Zugriffsrechte werden durch die Sektionen geregelt. Ausserdem ist auch der Zugriff auf die konsolidierten Daten geregelt und kontrolliert. Nur autorisierte Mitarbeitende des BFS erhalten einen solchen Zugriff.
Für Erhebungen von konsolidierten Daten mit überjährigen Periodizitäten werden bei jeder neuerlichen Durchführung neue Pseudo-Identifikatoren gebildet.

7.3 Pseudonymisierung und De-Pseudonymisierung

Pseudonymisierung
Die Pseudonymisierung besteht darin, alle direkt identifizierenden Personenmerkmale (z.B. Name, Adresse) von Einzeldatensätzen sowie die originären und übergreifenden Identifikatoren durch BFS-intern vergebene Pseudo-Identifikatoren zu ersetzen. Pseudonymisierte Datensätze lassen somit keine unmittelbaren Rückschlüsse auf Personen mehr zu.
Pseudo-Identifikatoren werden entweder durch einen Verschlüsselungsalgorithmus generiert (z.B. innerhalb von SIS) oder direkt vergeben (z.B. Zuteilung neuer Identifikatoren und Erstellen einer Übersetzungstabelle). Daten ausserhalb von SIS müssen auch mit dem in SIS verfügbaren Verschlüsselungsprogramm pseudonymisiert werden. Die Pseudonymisierung erfolgt innerhalb von SIS mittels eines zweistufigen Verfahrens (Stufe 1: BFS-Schlüssel, Stufe 2: sektorspezifischer Schlüssel) vom ursprünglichen Identifikator zum Pseudo-Identifikator.

Für jede Produktion (Erhebung) von konsolidierten Daten werden jeweils unterschiedliche Pseudo-Identifikatoren mit den entsprechenden Schlüsseln generiert. Mit diesem Vorgehen wird erreicht, dass sich Datensätze, die die gleiche Person oder Beobachtungseinheit betreffen, ohne zusätzliche Informationen nicht zusammenführen bzw. miteinander verknüpfen lassen.
Die für die Pseudonymisierung verwendeten Schlüssel (Algorithmen, Übersetzungstabellen) werden zur sicheren Aufbewahrung in einem speziell gesicherten Schlüsselschrank (nach dem Schlüsselschrankprinzip; siehe Kap.0) abgelegt und gleichzeitig an allen übrigen Orten gelöscht bzw. vernichtet. Die Schlüssel sind dann nur noch via Schlüsselschrank zugänglich. Die Schlüssel werden von der Sektion IT im Auftrag der Verknüpfungsstelle generiert und verwaltet.

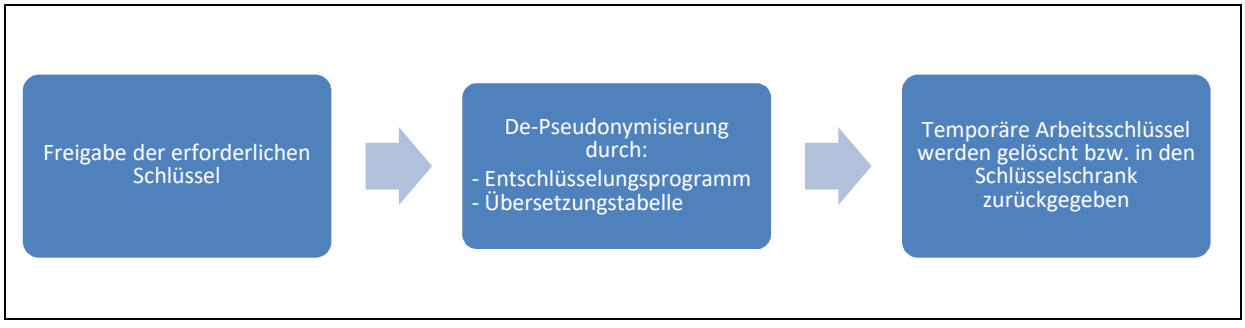
➔ Prozess Pseudonymisierung



De-Pseudonymisierung
Der umgekehrte Vorgang ist die De-Pseudonymisierung. Um Daten verschiedener Erhebungen/Sektoren miteinander verknüpfen zu können, müssen die jeweiligen Identifikatoren zuerst de-pseudonymisiert, also entschlüsselt, werden, sofern sie nicht aus dem gleichen Sektor stammen. Wenn Daten aus dem BFS verknüpft werden, betrifft die De-Pseudonymisierung nur eine Stufe (von Stufe 2 auf Stufe 1). Aus den pseudonymisierten Identifikatoren werden die ursprünglichen Identifikatoren wieder hergestellt und anschliessend durch einen projektspezifischen Identifikator ersetzt, mit denen die betroffenen Datensätze verknüpft werden können.

- Schlüssel wird aus Schlüsselschrank von der Sektion IT dem Sektorverantwortlichen zur Nutzung freigegeben
- Entschlüsselungsprogramm wird durchgeführt
- Pseudo-IDs werden mit Hilfe des Schlüssels durch ursprüngliche IDs ersetzt.
- Sektorverantwortlicher erstellt projektspezifischen Identifikator für Verknüpfung

➔ Prozess De-Pseudonymisierung



7.4 Prinzip des Schlüsselmanagements

Datenverknüpfungen kann nur vornehmen, wer über die dazu erforderlichen Schlüssel bzw. über entsprechende Zugriffsrechte verfügt. Die Kontrolle über die Datenverknüpfungen kann somit über eine gesicherte Aufbewahrung der Schlüssel im Schlüsselschrank und ein striktes zentrales Schlüssel-Management (Key-Management) erreicht werden.

Konzept:
Die Schlüssel werden zentral und gesichert im sogenannten ***Schlüsselschrank*** aufbewahrt. Der Schlüsselschrank ist eine BFS-weite Infrastruktur, die es der Sektion IT erlaubt, Schlüssel zu verwalten und Berechtigungen für die Nutzung der Schlüssel zu erteilen. Der Zugang zum Schlüsselschrank liegt im Verantwortungsbereich der Direktion (siehe Kap. 8) und ist implizit durch die Genehmigung der Verknüpfung im Gever-Prozess gewährleistet.
Die zentrale Infrastruktur des Schlüsselschranks mit den darin enthaltenen Schlüsseln sowie die Zugriffe hierauf werden durch die Sektion IT verwaltet. Die Sektion IT erteilt die jeweiligen Verwendungs- und Zugriffsrechte für die De-Pseudonymisierung und das Erstellen der Schlüssel an den jeweiligen Sektorverantwortlichen. Der Schlüsselschrank entspricht der von der Sektion IT entwickelten Lösung in der Informatica-Umgebung. Der Zugriff auf den Schlüsselschrank für die Sektion IT und die Sektorverantwortlichen ist geschützt (Login nur für berechtigte ETL-Prozesse).
Aus sicherheitstechnischen Gründen kann nur der Sektorverantwortliche mit der entsprechenden Autorisierung der Verknüpfungsstelle über die Sektion IT die De-Pseudonymisierung von Dateien aus seinem Sektor ausführen.
Die Sektion IT ist auch für die Verwaltung des neu angelegten Sektorenschlüssels des aus der Verknüpfung resultierenden Datensatzes verantwortlich. Ein wichtiger Grundsatz ist, dass die Sektion IT keinen Zugriff auf statistische Daten hat.

Eine Dokumentation der Informatica Pseudonymisierungsinfratstruktur (nur BFS-intern verfügbar) befindet sich unter https://intranet.confluence.bfs.admin.ch/confluence/pages/viewpage.action?pageId=27754683

8 Organisation und Rollen

Direktion

Die Direktion ist gemäss Art. 2 Abs. 3 der Datenverknüpfungsverordnung des EDI verantwortlich für die Verknüpfungen. Mit Direktion ist der BFS-Direktor gemeint. Er kann für seine Entscheide die Geschäftsleitung beratend beiziehen. Die Direktion ist Auftraggeberin und trifft den Entscheid über die Durchführung von Verknüpfungen und die allenfalls damit verbundenen Vorbehalte und Anforderungen. Mit der Autorisierung für eine Verknüpfung wird auch die Benutzung der dazu erforderlichen Verknüpfungsschlüssel definiert.

Arbeitsgruppe Verknüpfungen

Die Arbeitsgruppe Verknüpfungen (AG) wird durch ein Mitglied der Geschäftsleitung geleitet. In ihr haben mindestens ein Vertreter pro Abteilung, vom Rechtsdienst, der Sektion Statistische Methoden, von der Informatik und von der Verknüpfungsstelle Einsitz. Sie trifft sich bei Bedarf, mindestens aber zweimal jährlich.
Das Mandat für die Arbeitsgruppe wurde in der GL am 09. Dezember 2015 erteilt und sieht die folgenden Aufgaben vor:

Unterstützung, Diskussion und Evaluation der Arbeiten im Rahmen der Datenverknüpfungen mit den folgenden Themenschwerpunkten:

- Allgemeine und konzeptionelle Ausrichtung der Datenverknüpfungen und Monitoring der Arbeiten
- Operative Umsetzung/Organisation, einschliesslich Informatik (technisch, inhaltlich und organisatorisch)
- Rechtsgrundlagen, insbesondere Datenschutz und methodische Voraussetzungen

- Kommunikation und Transparenz (intern und extern)

Verknüpfungsstelle

Die Verknüpfungsstelle ist verantwortlich für

- die administrative Begleitung und die Koordination von Datenverknüpfungen. Dazu gehören insbesondere die formale Überprüfung der Anträge, die Zusammenstellung und Weiterleitung der internen Stellungnahmen (in Form einer synthetisierten Empfehlung), die Führung des Entscheidungsprozesses, die Steuerung, formale Überwachung und Dokumentation von Verknüpfungsvorhaben und die Erteilung von Auskünften bei Fragen. Die Verknüpfungsstelle darf keinen Zugriff auf zu verknüpfende Daten haben.
- Besprechung und Empfehlung bei speziellen Anträgen betreffend Inhalt, Methodik, Qualität, Machbarkeit und Ethik. Bei Bedarf werden weitere Stellen (Sektion Statistische Methoden, Rechtsdienst, Arbeitsgruppe Verknüpfungen, usw.) hinzugezogen.
- die Pflege des Inventars

Sektorverantwortliche[6]

Der/die Sektorverantwortliche ist verantwortlich für einen Sektor und nimmt folgende Aufgaben wahr:

- Er/sie verwaltet den Zugriff von autorisierten Personen auf den **Sektor**.
- Er/sie erhält die Rechte von der Verknüpfungsstelle, um die **Pseudonymisierung und die De-Pseudonymisierung** auszuführen. Er/sie ist verantwortlich für die Benutzung der **Schlüssel** für seinen Sektor. Er/sie ist die einzige Person, die die Verwendung der Schlüssel bei der Sektion IT beantragen kann.
- Er/sie ist zuständig für die Sicherstellung der Pseudonymisierung von **konsolidierten Daten**. Er/sie stellt auch sicher, dass der Zugriff auf die konsolidierten Daten nur durch autorisierte Personen erfolgt.

Der/die Sektorverantwortliche ist als Rolle zu verstehen, die innerhalb einer Organisationseinheit, z.B. zu Stellvertretungszwecken, mehreren Personen übertragen werden kann.

Sektormitarbeitende

Der/die Sektormitarbeitende ist eine Fachperson eines Sektors. Der/die Sektormitarbeitende erhält den Zugriff auf den Sektor und die konsolidierten Daten vom Sektorverantwortlichen.
Der/die Sektormitarbeitende ist als Rolle zu verstehen, die innerhalb einer Organisationseinheit, z.B. zu Stellvertretungszwecken oder zur Erfüllung gemeinsamer Arbeiten, mehreren Personen übertragen werden kann.

Weitere Rollen

- Abteilungsleitung: Die Leitung der betroffenen Abteilung ist die erste Entscheidungsinstanz bei internen und externen Verknüpfungsanträgen. Sie stellt die fachliche Beurteilung sicher und stellt allfällig benötigte Ressourcen für die Verknüpfung zur Verfügung.
- Rechtsdienst: prüft die internen und externen Verknüpfungsanträge aus rechtlicher Sicht.
- Sektion Statistische Methoden: prüft die internen und externen Verknüpfungsanträge hinsichtlich der statistisch-methodischen Machbarkeit und Korrektheit.
- Sektion Informatik: erledigt im Auftrag der Verknüpfungsstelle das Schlüssel-Management und insbesondere die Zugangsverwaltung zum Schlüsselschrank. Eine begrenzte Anzahl von Personen bei der der Sektion IT[7] ist verantwortlich für das Schlüssel-Management. Diese Personen sind befugt, basierend auf einem Direktionsentscheid die erforderlichen Verknüpfungsschlüssel den Sektorverantwortlichen für die De-Pseudonymisierung zugänglich zu machen,

[6] Wenn in der Folge von Sektorverantwortlichen oder Sektormitarbeitenden gesprochen wird, ist das im Sinne von Rollen und beispielsweise damit verbundenen Zugriffsrechten zu verstehen. Es ist durchaus möglich, dass eine einzige Person gleichzeitig mehrere Rollen wahrnimmt.
[7] Es handelt sich um die "Keystore Verantwortlichen" des Teams INFA des IT-CORP Dienstes.

resp. entsprechende Zugriffsrechte zu erteilen. Das Schlüssel-Management wacht zudem über die korrekte Verwendung und die eingeschränkten Nutzungsberechtigungen der Schlüssel nach Abschluss der Verknüpfungen. Die Sektion IT hat keinen Zugriff auf Einzeldaten.

9 Elemente der Datenverknüpfung

9.1 Inventare der Verknüpfungen im BFS

Sämtliche Verknüpfungen im BFS sind einer der vier Verknüpfungskategorien zugewiesen (siehe Kap. 6.1.2) . Die Übersicht über alle Verknüpfungen wird im BFS durch Inventare sichergestellt. Damit sind Transparenz und die Anliegen des Datenschutzes erfüllt. In Kap. 6.3 sind die Voraussetzungen pro Verknüpfungsart definiert.

Verknüpfungen für die Statistikproduktion

Die Verknüpfungen für die Statistikproduktion sind in der Erhebungsverordnung aufgeführt. Dieses Inventar der Öffentlichen Statistik hat sich gut bewährt und ist entsprechend bekannt. Die Verknüpfungen des Produktionsprozesses wurden 2014 im Rahmen der jährlichen Anpassung der Statistikerhebungsverordnung in den Beschreibungen zu den Erhebungen ergänzt.

- Gefäss: Erhebungen oder Statistiken sind sowohl im Anhang der Statistikerhebungsverordnung als auch im Inventar der Produktionsverknüpfungen aufgeführt und öffentlich zugänglich über BFS-Homepage
- Verantwortlichkeit für die Durchführung: Rechtsdienst
- Verfahren: Jährlicher Revisionsprozess des Anhanges zur Verordnung. Die fachlichen Organisationseinheiten (Sektoren) beantragen die Verknüpfungen laufend. Antragsprozess gemäss dieser Verknüpfungsrichtlinie (siehe Kap. 10 und Anhang 5).
- Bewilligung: Entscheid Direktion sowie Bundesrat über Inkraftsetzung der Verordnung.

Längsschnittverknüpfungen

Längsschnittverknüpfungen sind in der Regel weniger heikel als Querschnittsverknüpfungen, da das Zusammenfügen von Daten der gleichen Erhebung aber mit unterschiedlichem Erhebungszeitpunkt naheliegend ist. Nichtsdestotrotz können auch hier sensible Profile entstehen. Deshalb müssen auch Verknüpfungen für Längsschnittverknüpfungen lückenlos aufgeführt und bewilligt werden.

- Gefäss: Inventar über die Datenverknüpfungen
- Verantwortlichkeit der laufenden Nachführung: Verknüpfungsstelle
- Verfahren: die Sektoren beantragen laufend die Längsschnittverknüpfungen bei der Verknüpfungsstelle. Antragsprozess gemäss diesem Dokument (siehe Kap. 10 und Anhang 5)
- Bewilligung: Entscheid Direktion (der Direktor kann die GL konsultieren)

Verknüpfungen für Datenanalysen

Die Verknüpfungen für Datenanalysen sind in der Regel nicht systematisch im Sinne von wiederkehrend. Die Anfragen auf Verknüpfung von Daten können BFS-intern oder von Dritten erfolgen. Mit der Inkraftsetzung der Datenverknüpfungsverordnung des EDI (siehe Anhang 2, Punkt 4) werden die Anfragen von der Verknüpfungsstelle dokumentiert.

- Gefäss: Inventar über die Datenverknüpfung
- Verantwortlichkeit der laufenden Nachführung: Verknüpfungsstelle
- Verfahren: Anträge werden laufend gestellt und gemäss dem Prozess in dieser Verknüpfungsrichtlinie durch die Verknüpfungsstelle bearbeitet (siehe Kap. 10 und Anhang 5)
- Bewilligung: Entscheid Direktion (der Direktor kann die GL konsultieren)

Spezialfälle

Alle Verknüpfungen, welche nicht in einer der drei oben aufgeführten Verknüpfungsarten inventarisiert sind, werden ebenfalls im Inventar geführt. Ziel ist es, die Vollständigkeit über alle Verknüpfungen sicherzustellen.

- Gefäss: Inventar über die Verknüpfung von Spezialfällen, nicht öffentlich zugänglich
- Verantwortlichkeit der laufenden Nachführung: Verknüpfungsstelle
- Verfahren: Laufender Antrag an die Verknüpfungsstelle
- Bewilligung: Entscheid Direktion (der Direktor kann die GL konsultieren)

8.2 Verknüpfungsanträge

Verknüpfungsbegehren sind schriftlich einzureichen (siehe auch Anhang 5) und erfolgen in der Regel über die zentrale Verknüpfungsstelle oder eine betroffene Fachsektion. Wird ein solches Begehren über eine Fachsektion eingereicht, ist umgehend die Verknüpfungsstelle einzubeziehen.

Erforderliche Angaben

Die Verknüpfungsstelle prüft beim Eingang des Antrages die Dokumentation auf Vollständigkeit (Antragsformular vollständig ausgefüllt sowie je nach Anfrage Forschungsauftrag, Variablenbeschreibungen, etc.). Ein Verknüpfungsantrag enthält unabhängig von der Verknüpfungskategorie die nachfolgenden Informationen:

- Informationen zum Antragsteller (Person, Institution)
- Beschreibung des Vorhabens (inkl. Ziel und Zweck der Verknüpfung)
- Erforderliche Daten (zu verknüpfende Daten, Merkmale; im Falle von externen Daten auch Metainformationen und Rechtsgrundlagen)
- Angestrebte Ergebnisse (allenfalls auch geplante Publikation)
- Termine
- Zusätzliche Angaben (Art der Verknüpfung wie z.B. erst-/einmalige oder wiederkehrende Verknüpfung, spezielle IT-Tools oder Programme).

Dokumentation:

Alle Verknüpfungsanträge und die durchgeführten Verknüpfungen werden dokumentiert. Bestandteil der Dokumentation sind: •Antrag •Beurteilung •Entscheid •Datenschutzvertrag oder Bearbeitungsreglement je nach Schutzstufe und Verknüpfungsart
Die Dokumentation wird in GEVER geführt.

Systematische Verknüpfungen für die Statistik-Produktion und Längsschnittverknüpfungen

Datenverknüpfungen für die Statistikproduktion sowie Längsschnittverknüpfungen sind im Anhang der Erhebungsverordnung aufgeführt. Sie müssen wie alle übrigen Verknüpfungen dokumentiert und vom Direktor bewilligt werden (siehe Verfahren 9.1). Solche Verknüpfungen werden in der Regel bei der Verabschiedung der entsprechenden Konzepte genehmigt und anschliessend im Anhang zur Erhebungsverordnung rechtlich abgestützt und bei Schutzstufe 3 im dazugehörenden Bearbeitungsreglement dokumentiert.

Wiederholte Verknüpfungsbegehren

Bei Verknüpfungsanträgen, die in gleicher oder ähnlicher Form bereits einmal eingereicht worden sind, kann auf die früheren Unterlagen verwiesen werden. Auf allfällige Unterschiede ist explizit und ausreichend detailliert hinzuweisen.

Bewilligungsdauer

- Verknüpfungen für die Statistikproduktion: Die Autorisierung und der Zugang zu den erforderlichen Identifikatoren bzw. Schlüsseln kann bei solchen systematischen Verknüpfungen für eine bestimmte Zeitdauer erteilt werden. Entsprechende Bewilligungen sind periodisch zu erneuern. Im jeweiligen Antrag ist die gewünschte Zeitdauer aufzuführen; sie kann maximal fünf Jahre betragen (siehe auch Kap. 10.2.2).
- Verknüpfungen für Externe: Die Dauer der Datennutzung ist vertraglich definiert. Eine Verlängerung kann gegebenenfalls beantragt werden.

9.3 Bearbeitungsreglement

Wie in Kap. 5 erläutert, braucht es für die Verknüpfung als solche - zusätzlich zu den vorliegenden Richtlinien und den gesetzlichen Vorgaben - keine spezifischen Bearbeitungsreglemente. Ob ein spezifisches Bearbeitungsreglement erforderlich ist, hängt vielmehr von der Schutzstufe der Input- und Output-Daten ab. Sind die Input-Daten der Schutzstufe 3 zuzuordnen, bestehen bereits Bearbeitungsreglemente für die entsprechenden Datensammlungen, die die Datensicherheit regeln und insbesondere den willkürlichen Zugriff auf die Daten verunmöglichen. Ein zusätzliches spezifisches Bearbeitungsreglement für deren Verknüpfung ist deshalb nicht nötig. Die verknüpfungsspezifischen Angaben müssen aber transparent dokumentiert werden. Namentlich muss im Antragsformular definiert werden, welche Variablen genau verknüpft werden sollen und wer wie lange Zugriff auf die de-pseudonymisierten Daten hat. Werden Daten der Schutzstufen 0-2 verknüpft, besteht in der Regel noch kein Bearbeitungsreglement. In diesen Fällen ist anhand der Schutzbedarfsanalyse (Schuban) zu entscheiden, ob für die neu entstehende Datensammlung (verknüpfte Daten) ein Bearbeitungsreglement notwendig ist. Dies ist dann der Fall, wenn die verknüpften Daten (Output-Daten) der Schutzstufe 3 zuzuordnen sind.

Das Template "Bearbeitungsreglement für Erhebungen (Datensammlungen) der Schutzstufe 3", inklusive Modul "Verknüpfung", befindet sich im Anhang 3.

9.4 Einbezug Dritter in die Verknüpfungsarbeiten

Gemäss Art. 13*k* Abs. 3 Erhebungsverordnung können Dritte (BFS-externe Personen) in den Verknüpfungsprozess einbezogen werden, wenn das BFS aus Knowhow-, Ressourcen- oder Effizienzgründen die Arbeiten nicht selbständig erledigen kann. Das De-Pseudonymisieren und Erstellen des projektspezifischen Identifikators wird immer durch das BFS erledigt. Um beim Einbezug von Dritten in weitere Prozessschritte Datenschutz und Datensicherheit zu gewährleisten, trifft das BFS die nötigen organisatorischen und technischen Vorkehrungen (siehe auch Kap. 10.3.2). In gewissen Fällen macht es aus organisatorischen Gründen oder zur Einhaltung des Datenschutzes Sinn, diese Arbeiten innerhalb des BFS an einem gesicherten Arbeitsplatz durchführen zu lassen.

Organisatorische Vorkehrungen

- Mit den mitwirkenden Dritten wird vor Aufnahme ihrer Verknüpfungstätigkeit eine gegenseitig unterzeichnete schriftliche Vereinbarung getroffen, worin das Vorgehen, Rechte und Pflichten sowie die Datenschutzbestimmungen detailliert festgehalten sind (Vertrag Typ 2).
- Die Sektorverantwortlichen sorgen dafür, dass die projektspezifischen Identifikatoren (siehe 10.3.1) und die für die Verknüpfung benötigten Daten in geeigneter Form bereitgestellt werden.
- Falls Dritte gewisse Arbeiten im BFS vornehmen müssen: Empfang und Einweisung der externen Verknüpfer sowie Abschluss der Aktion mit den Abschlussformalitäten und der Überlassung der verknüpften Daten (mit entsprechendem Datenschutzvertrag) werden durch die Sektorverantwortlichen wahrgenommen.
- BFS Fachpersonal steht für eine zeitlich begrenzte Beratung und Unterstützung zur Verfügung.

Technische Vorkehrungen

Im Fall von Verknüpfungsarbeiten im BFS: es werden im BFS speziell ausgerüstete Arbeitsplätze mit entsprechendem Keystore durch die IT zur Verfügung gestellt. Dabei werden die folgenden Vorkehrungen getroffen:

- Der Arbeitsplatz ist mit einem PC ausgerüstet, der über die benötigten Kapazitäten und Software verfügt. Das Gerät verfügt über keinerlei Verbindungen oder Schnittstellen zur „Aussenwelt“. Für die mitwirkenden Dritten bestehen somit keinerlei Möglichkeiten Daten über technische Schnittstellen (USB, CD etc.) zu exportieren. Es gibt auch keine Verbindung zu irgendwelchen Netzwerken (Internet, Intranet, eMail etc.).
- Die für die Verknüpfung benötigten Daten (Input-Daten) können jederzeit über die USB-Schnittstelle auf die Maschine importiert werden. Die erstellten verknüpften Daten (Output-Daten) können nur durch den zuständigen Systemadministrator exportiert werden. Für den Export ist die Intervention eines OSS des BIT notwendig.

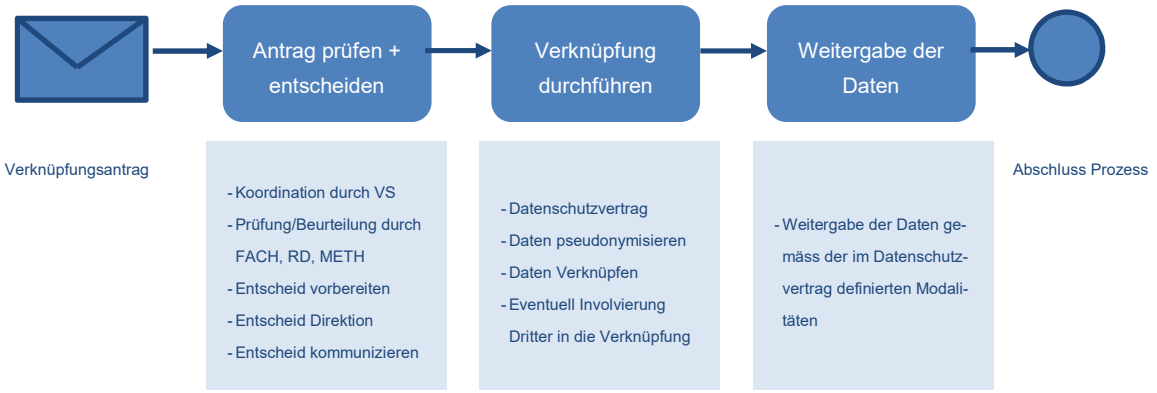
Die Nutzung solcher geschlossenen Arbeitsplätze wird auf das Minimum reduziert.

10 Verknüpfungsprozesse

(siehe auch Anhang 4 Prozessbeschreibung)

10.1 Einleitende Bemerkungen

Bei der Abwicklung von Verknüpfungen wird nach folgendem Basisprozess vorgegangen:



Im Wesentlichen werden fünf Schritte unterschieden:

- Verknüpfungsantrag bzw. Verknüpfungsanfrage,
- Prüfung des Antrags mit dem Entscheid ob, wie und wann eine Verknüpfung durchgeführt werden kann,
- Durchführung der Verknüpfung,
- Weitergabe der verknüpften Daten,
- Abschluss des Verknüpfungsprozesses.

10.2 Antrag prüfen und entscheiden

10.2.1 Antrag prüfen

Die Beurteilung eines Verknüpfungsbegehrens bei externen Anfragen wird durch die betroffenen Fachsektionen (FACH, bei internen Anfragen genügt der von der Abteilungsleitung unterschriebene Antrag), die Sektion Statistische Methoden (METH) und den Rechtsdienst (RD) vorgenommen (siehe auch Art. 2 Abs. 2 Datenverknüpfungsverordnung).

Die Stellungnahmen werden durch die zentrale Verknüpfungsstelle koordiniert. Sie setzen sich zusammen aus zwei Teilen:

1) Bereichsspezifische Beurteilung des Vorhabens.
2) Antrag bzw. Empfehlung zuhanden der Entscheidungsinstanz.

Als erstes wird der Antrag an die verantwortliche Abteilungsleitungen zur Information weitergeleitet. Anschliessend machen die betroffenen Fachsektionen (FACH) die Beurteilung. Dies geschieht parallel zur Bearbeitung durch METH und RD zur methodischen und rechtlichen Beurteilung des Vorhabens. Das Ergebnis wird im Formular „Antrag, Beurteilung und Entscheid“ schriftlich festgehalten. Die Stellungnahmen von FACH, METH und RD werden von der Verknüpfungsstelle zusammengefasst und an die verantwortliche Abteilungsleitungen weitergeleitet, die den Antrag der Geschäftsleitung unterbreiten. Ohne Einspruch eines Geschäftsleitungsmitglieds geht das Dokument an die Direktion zwecks Entscheid.

Bei Verknüpfungsbegehren von anderen Bundesämtern ist in jedem Falle mit dem Antragsteller Kontakt aufzunehmen, um das Vorhaben rasch zu klären und ein geeignetes Vorgehen zu vereinbaren.

Beurteilungen

Stellungnahme VERKNÜPFUNGSSTELLE: Ist der Antrag vollständig? Bemerkungen?

Beurteilung FACH: Sind die Daten und Identifikatoren vorhanden? Ist die Verknüpfung inhaltlich sinnvoll / zielführend? Ist die Verknüpfung machbar (methodisch, technisch)? Wie sensibel sind die Daten (Input / Output)? Verknüpfungsaufwand / Ressourcenlage? Vorgehen (wer macht was, wann und wie)? Bedingungen, Vorbehalte / Restriktionen (spez. Vorkehrungen, Umgang mit Output-Daten, …)?

Beurteilung METH: Ist das Vorhaben methodisch korrekt/vertretbar? Machen die Ergebnisse Sinn? Vorbehalte/Restriktionen?

Beurteilung RD: Sind die rechtlichen Voraussetzungen gegeben? Beurteilung der Sensibilität (Input-Daten + Ergebnisse), Vorbehalte, besondere Anforderungen/Vorkehrungen.

In gewissen seltenen Fällen (z.B. Speicherung der Daten auf einer Cloud) wird zusätzlich eine *Beurteilung der Sektion IT* benötigt.

(⇨siehe Anhang 5 Formular)

10.2.2 Entscheid der Direktion

Auf der Basis des Antrags bzw. der Empfehlung der beurteilenden Instanzen entscheidet die Direktion darüber, ob, in welcher Form und mit welchen Vorbehalten (z.B. besondere Massnahmen, zusätzliche Anforderungen, Vorbehalte bezüglich Weiterverwendung, Aufbewahrung, Löschung der Daten, Vorbehalte bzgl. Terminplanung) bzw. Erleichterungen eine Verknüpfung durchgeführt werden darf.

- Die Entscheide werden schriftlich festgehalten.
- Der Antragsteller wird von der federführenden Sektion schriftlich über den Entscheid und die Beurteilung informiert. Im Falle einer Ablehnung, werden die Gründe dargelegt.
  Wird ein Antrag abgelehnt und ist die Begründung für die Antragsteller nicht nachvollziehbar, kann eine Wiedererwägung beantragt werden.
- Ein positiver Direktions-Entscheid (in Schriftform) autorisiert die *Sektion IT* unter Berücksichtigung der Vorbehalte die für die Verknüpfung benötigten Schlüssel freizugeben bzw. zu generieren und freizugeben.

(⇨siehe Anhang 5 Formular)

Mögliche Vorbehalte und Erleichterungen beim Direktionsentscheid:

Vorbehalte:
Bei besonders sensiblen bzw. schützenswerten Daten kann verlangt werden, dass

- besondere (Sicherheits-) Massnahmen bei der Verknüpfungsdurchführung getroffen werden,
- besondere Einschränkungen bezüglich der Datenweitergabe oder der Datennutzung gemacht werden.

Bei Verknüpfungen, die einen grösseren Aufwand verursachen oder ein spezifisches Know-how erfordern, kann verlangt werden, dass sie unter bestimmten Voraussetzungen (siehe 10.3.2) durch den Antragsteller selbst durchgeführt werden.

Erleichterungen:

- Bei Anträgen, die die Integration einer Verknüpfung in eine systematisch wiederkehrende Statistikproduktion betreffen, kann eine „Dauerbewilligung“ erteilt werden. Die Dauer richtet sich nach der Art der Statistikproduktion und nach der Sensibilität der Daten. Deren Festlegung liegt im Ermessen der Direktion.
- Je nach Sensibilität der Daten, Typ des Antragstellers oder Verknüpfungsbegehren sind Vereinfachungen des Verfahrens zulässig. Sie liegen im Ermessen der Direktion.

10.3 Durchführung der Datenverknüpfung

Die Federführung für die Durchführung einer Verknüpfung liegt bei der Sektion, die für die involvierten Daten zuständig ist. Sind mehrere Sektionen betroffen, einigen sich diese über die Federführung, Rollen und Verantwortlichkeiten.

10.3.1 Verknüpfung durch das BFS

Im Normalfall werden Verknüpfungen durch das BFS vorgenommen. Das De-Pseudonymisieren und Erstellen des projektspezifischen Identifikators werden immer durch das BFS durchgeführt. Die Verknüpfung geschieht idealerweise gemäss den folgenden Schritten:

- ***Daten bereitstellen:***

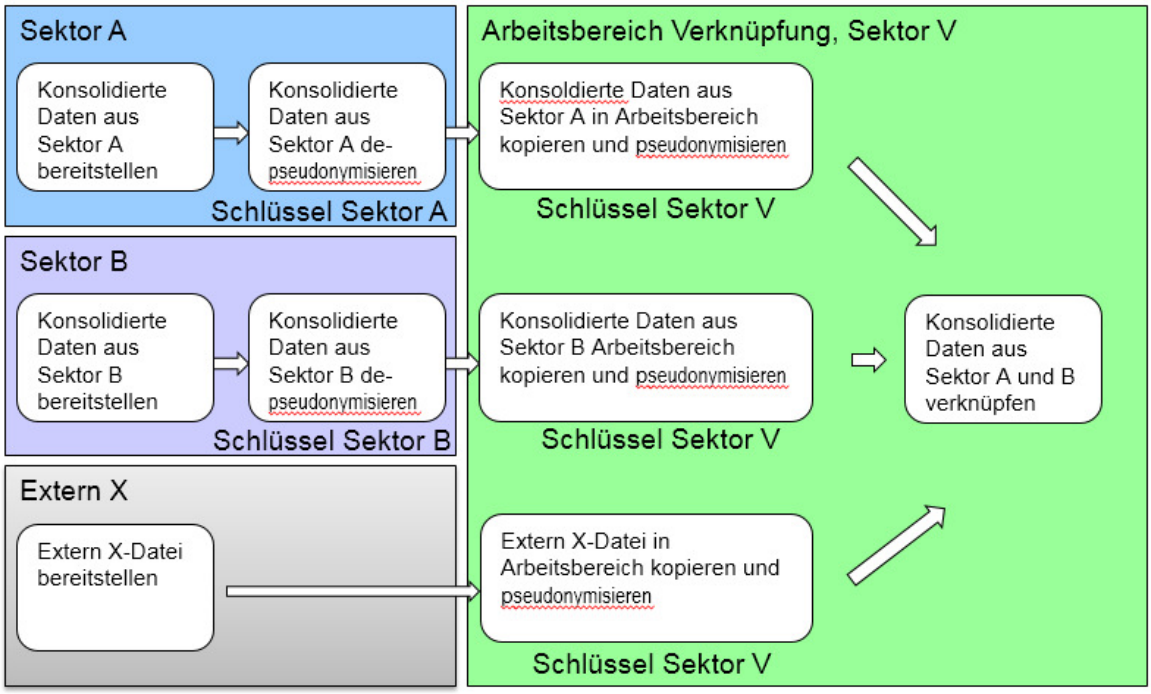
  BFS-Daten werden aus den jeweiligen Datenpools extrahiert und in einem speziellen Arbeitsbereich, welcher durch die Sektion IT vorbereitet wurde, für die Verknüpfung bereitgestellt.

- ***Daten de-pseudonymisieren:***

  Die bereitgestellten pseudonymisierten BFS-Daten können mit Hilfe der durch die Verknüpfungsstelle freigegebenen Schlüssel de-pseudonymisiert werden.

- ***Daten verknüpfen und pseudonymisieren:***

  Die Daten werden in der Informatica-Umgebung pseudonymisiert. Mit Hilfe der gemeinsamen projektspezifischen Identifikatoren können die Einzeldaten miteinander verbunden werden.



Diese Darstellung gibt die Verantwortungsbereiche der einzelnen Sektoren wieder, jedoch nicht physische Ablagen oder Datenbanken. Für diese wäre ein solches Schema falsch, weil pseudonymisierte und de-pseudonymisierte Daten nicht auf der gleichen Ablage liegen dürfen.

Eine Dokumentation der Informatica Pseudonymisierungsinfratstruktur (BFS-intern) befindet sich unter https://intranet.confluence.bfs.admin.ch/confluence/pages/viewpage.action?pageId=27754683

10.3.2 Einbezug Dritter in den Verknüpfungsprozess

Aus Aufwand-, Effizienz- oder Know-how Gründen können externe Personen in den Verknüpfungsprozess einbezogen werden (siehe Art. 13*k* Abs. 3 Statistikerhebungsverordnung). Diese Mitwirkung von Dritten ist vertraglich zu regeln (vgl. Datenschutzvertrag Typ 2).

Daten bereitstellen:

Die für die Verknüpfung erforderlichen BFS-Daten werden durch die verantwortlichen Mitarbeiter des BFS de-pseudonymisiert und bereitgestellt.

BFS-externe Daten (Dritt- oder Fremddaten) werden im BFS entgegengenommen und durch die verantwortlichen Mitarbeiter des BFS bereitgestellt.

Diese Daten (BFS-Daten sowie Fremd- oder Drittdaten) enthalten einen für die Verknüpfung geeigneten Identifikator.

Die ursprünglichen Identifikatoren werden in einen neuen, projektspezifischen Identifikator umgewandelt. Die so pseudonymisierten Daten werden über einen gesicherten Kanal an die Datennutzer übermittelt.

Daten konkret verbinden:

Mit Hilfe des gemeinsamen projektspezifischen Identifikators können die Einzeldaten durch die externen Personen miteinander verbunden werden. Es wird ein File mit den verknüpften Einzeldaten erstellt.

In begründeten Fällen: Arbeitsplatz für externe Mitwirkende bereitstellen: (siehe Kap. 9.4)

In gewissen Fällen ist es aus technischen Gründen notwendig, dass Dritte direkt im BFS gewisse mit der Verknüpfung in Zusammenhang stehenden Aufgaben wahrnehmen. Dies ist zum Beispiel

der Fall, wenn Dritt- oder Fremddaten keinen für die Verknüpfung geeigneten Identifikator enthalten und zeitaufwendige probabilistische Verfahren oder manuelle Schritte angewendet werden. Ein konkretes Beispiel wäre die Personensuche anhand der Kriterien *Vorname, Name und Wohngemeinde*: dieses Verfahren setzt die Entwicklung einer Methode und gegebenenfalls gewisse manuelle Selektionen voraus, welche zeitaufwändig sind und in der Verantwortung der Datennutzer liegen. Sind solche Verknüpfungsarbeiten im BFS durch die externen Personen abgeschlossen, werden die Ergebnisse durch die federführende Fachsektion gegebenenfalls noch pseudonymisiert und auf jeden Fall geprüft. Insbesondere werden die folgenden Fragen geklärt:

- Wurden die Arbeiten wie vertraglich vereinbart durchgeführt?
- Entspricht das Ergebnis-File dem vertraglich vereinbarten Output?

Durch das BFS nicht im Detail geprüft wird die inhaltliche und methodische Korrektheit der verknüpften Daten, die in der Verantwortung der Antragsteller liegt.

Unabhängig davon, ob gewisse Arbeitsschritte von Dritten übernommen werden (im BFS oder nicht), sind die den Datennutzern schlussendlich gelieferten Daten ausnahmslos wie unter 10.3.1 beschrieben pseudonymisiert.

10.3.3 Verknüpfung durch kantonale oder kommunale Verknüpfungsstellen

Dem Begehren einer kantonalen oder kommunalen Statistikstelle, selbst eine Verknüpfung mit Daten aus der Bundesstatistik – auch in nicht pseudonymisierter Form – durchzuführen, kann unter bestimmten Voraussetzungen entsprochen werden (siehe Art. 14*a* Abs. 2 BstatG, Art. 13*j* Abs. 4 Statistikerhebungsverordnung und Art. 5 Datenverknüpfungsverordnung des EDI). Sind diese erfüllt und liegt ein adäquates Bearbeitungsreglement und ein gegenseitig unterzeichneter Verknüpfungs- und Datenschutzvertrag vor, hat die federführende Fachsektion nur noch die Rolle, allenfalls benötigte Daten (mit geeignetem Identifikator) zu liefern und zu verifizieren, dass die vertraglichen Abmachungen bezüglich Datenschutz und Datennutzung eingehalten werden.

10.4 Weitergabe verknüpfter Daten

Bezüglich der Weitergabe von verknüpften Daten gelten die gleichen Bestimmungen wie für die Weitergabe aller übrigen Einzeldaten. Massgeblich ist dabei, neben den Bestimmungen in Gesetz und Verordnung, insbesondere die „*Wegleitung zum Datenschutz bei der Weitergabe von Einzeldaten an Dritte*“ (Stand: 18.10.2006).

Einzelheiten zur Weitergabe von Einzeldaten sind immer in einem Datenschutzvertrag zu regeln.

10.5 Abschluss eines Verknüpfungsvorhabens und Löschung verknüpfter Daten

Liegen die verknüpften Daten vor und sind sie der vereinbarten Nutzung zugeführt, ist der Verknüpfungsprozess abgeschlossen. Formale Anforderungen sind noch:

- Die Rückgabe bzw. Löschung der von der Sektion IT erhaltenen Berechtigung zur Nutzung der Verbindungsschlüssel.

(siehe Anhang 5 Formular)

Im Interesse des Datenschutzes sind verknüpfte Daten nach Abschluss der Auswertungsarbeiten zu *vernichten*, wenn sie *Persönlichkeitsprofile* oder *besonders schützenswerte Daten* enthalten (siehe Art. 13m Statistikerhebungsverordnung). Der Entscheid, ob eine Vernichtung bzw. Löschung vorzunehmen ist, wird im Rahmen des Verknüpfungsentscheids (siehe Kap. 10.2.2) getroffen und unter „Spezifikationen, Vorbehalte“ festgehalten.

Sonderfaktoren

Es gibt mehrere Faktoren, die das konkrete, detaillierte Vorgehen beeinflussen können und bei der Beurteilung einer Verknüpfung zusätzlich eine Rolle spielen. Solche Faktoren sind insbesondere:

▶ ***Antragsteller.*** Diesbezüglich wird unterschieden nach:

- BFS-interne Antragsteller (Organisationseinheiten des BFS),
- BFS-externe Antragsteller (z.B. andere Bundesstellen, kantonale und kommunale Stellen, Forschungsinstitute, Dritte),
- Kantonale und kommunale statistische Ämter, die als Verknüpfungsorgane selbst Verknüpfungen durchführen wollen.

▶ ***Zu verknüpfende Daten*** (z.B. Art, Herkunft, Sensibilität der Daten). Hinsichtlich der Herkunft wird unterschieden nach (siehe auch Anhang 1 Definitionen (SIS-Konzepte)):

A) Daten des BFS (Daten über die das BFS die Datenherrschaft hat) ⇨ ***BFS-Daten***.

B) Daten, die im Rahmen des BStatG und der Statistikerhebungsverordnung erhoben worden sind, die aber nicht der Datenherrschaft des BFS unterstehen (z.B. Daten anderer Bundesämter) ⇨ ***Drittdaten***[8].

C) Daten, die ausserhalb des BStatG erhoben worden sind (z.B. Administrativdaten von Verwaltungsstellen oder Behörden; von Forschern oder andern Dritten selbst erhobene Daten) ⇨ ***Fremddaten***.

Aus diesen drei Daten-Typen sind die nachfolgenden ***Kombinationen*** / Verknüpfungen zulässig:

• **A** mit **A** • **A** mit **B** • **A** mit **C** • **B** mit **B** • **B** mit **C**

Nicht unter die vorliegenden Regelungen fallen Verknüpfungen C mit C. Dazu sind andere Rechtsgrundlagen erforderlich. Solche Verknüpfungen werden im BFS nicht durchgeführt.

Durch die Kombination dieser unterschiedlichen Faktoren ergibt sich eine Palette von zahlreichen denkbaren Varianten. Es ist nicht zielführend, sämtliche mögliche Vorgehens-Varianten detailliert zu beschreiben, weshalb nachfolgend jeweils eine „Standardvariante“ beschrieben wird und dazu Ergänzungen zu möglichen Abweichungen bzw. Spezialitäten dargestellt werden.

[8] Im SIS-Konzept wird nur von Fremddaten gesprochen. Im Anhang zur Statistikerhebungsverordnung werden zusätzlich Drittdaten definiert.

11 Anhänge

11.1 Anhang 1: Definitionen (SIS-Konzepte)

Definitionen ***(SIS Konzepte Seite 48 – 51 / 148)***

Entsprechend der Wertschöpfungskette werden folgende Bereiche gemäss SIS definiert:

Inputdaten
Unter Inputdaten (auch als Rohdaten bezeichnet) werden diejenigen Daten verstanden, welche durch Datenlieferanten und eigene Erhebungen von aussen geliefert und durch das BFS akzeptiert worden sind. Ihr wesentliches Merkmal ist, dass sie genau den angelieferten Zustand aus dem Kanal wiedergeben und noch nicht bearbeitet sind. Sie werden in dieser Rohform direkt gespeichert, damit sie für Rückverfolgungszwecke wieder hervorgeholt werden können.

Üblicherweise werden Inputdaten im BFS als Primärdaten (d.h. Daten für Statistik-Zwecke) und Sekundärdaten (d.h. Daten, die ursprünglich für andere Zwecke erfasst wurden, aber auch für statistische Zwecke verwendet werden) unterschieden. Beide Datenkategorien gehören zu den Inputdaten.

Für unsere Betrachtung ist jedoch ein anderes Kriterium massgebend, nämlich der Datenverantwortliche. Hier sind folgende zwei Arten von Inputdaten zu unterscheiden:

a) *(eigene) Erhebungsdaten*:
   Diese Daten werden durch das BFS oder externe Institutionen im Auftrag des BFS erhoben. Diese Daten stehen dem BFS als Rohdaten zur Verfügung und können/müssen durch das BFS kontrolliert und validiert werden.
   Diese Daten werden teils den Primärdaten zugerechnet (eigene Erhebungsdaten für Statistik-Zwecke), teils den Sekundärdaten (insbesondere die Register, welche das BFS selber führt).

b) *(fremde) Erhebungsdaten und externe Daten*:
   Diese Daten wurden nicht durch das BFS oder beauftragte Stellen erhoben, sondern z.B. durch andere Bundesämter, öffentliche Institutionen usw. Meistens werden sie in bereits verarbeiteter Form (validiert, seltener auch aggregiert oder anderweitig bearbeitet) geliefert.
   Da diese Daten ursprünglich nicht für statistische Zwecke erhoben wurden, sind sie in statistischer Hinsicht oft nicht vollständig; das BFS vervollständigt sie in diesem Fall in eigener Regie. Bereits bearbeitete (vor allem aggregierte) externe Daten dagegen können meist nicht mehr validiert werden.
   Zu diesen "Fremddaten" gehören sowohl alle nicht durch BFS bzw. BFS-Beauftragte erfassten Primärdaten sowie alle (nicht statistik-orientierten) Sekundärdaten. Im weiteren Sinne gehören zu den Inputdaten auch Produktdaten sowie Informationsobjekte von externen Datenlieferanten.

Da diese (für Statistikzwecke veränderten) Daten nun aber nicht mehr dem ursprünglichen Lieferanten gehören, wird das BFS in allen Fällen Datenherr über diese Daten, aber nur für deren statistische Verwendung.

Konsolidierte Daten
Konsolidierte Daten sind immer Einzeldaten bzw. Mikrodaten.

Dazu zählen die fertig aufbereiteten und pseudonymisierten Mikrodaten, ggf. erweitert um berechnete/abgeleitete Daten (z.B. Alter aus Geburtsdatum). Zu den Konsolidierten Daten gehören ebenfalls die Zwischenstände (A_0 .. A_n, F) gemäss der SDAP-Definition.

Konsolidierte Daten enthalten *keine aggregierten Werte*.

Zu den Konsolidierten Daten zählen auch individuell aufbereitete Mikrodaten, wobei diese durch besondere Massnahmen geschützt sind.

Physisches Format:
Konsolidierte Daten werden in Form von einer gewöhnlichen relationalen oder einer multidimensionalen Tabelle pro Erhebung im Data Pool abgelegt. Andere Formate werden anlässlich der Konsolidierung in diese Darstellung umgewandelt.
Dies erlaubt die korrekte Darstellung aller heute bekannten Inputformate, reduziert jedoch die Anzahl der für die weitere Verarbeitung notwendigen Formatvarianten (und damit die Anzahl von Transformationen anlässlich des Aufbaus von Data Marts für die Analyse). Ein weiterer, realisierungstechnischer Grund ist die Vorgabe, dass im Data Pool ausschliesslich Oracle (d.h. eine rein relationale Datenbank) verwendet werden soll.

Hinweis: In der Regel weisen konsolidierte Daten bereits in diesem Stadium multidimensionale Eigenschaften auf. Die Implementierung soll ermitteln, ob eine (normalisierte) Darstellung als Star-Schema/ Snowflake-Schema oder eine (nicht-normalisierte) Darstellung als flache Tabelle im Hinblick auf den Extraktions- und Umwandlungsaufwand in Cubes/Data Marts effizienter ist. Auf keinen Fall jedoch darf eine hersteller-spezifische Darstellung verwendet werden, da solche bei Konversion in andere Darstellungen erfahrungsgemäss immer Probleme verursachen.

Produktdaten
Produktdaten sind grundsätzlich das Ergebnis einer (in manchen Fällen automatisch durchgeführten) Analyse / Interpretation und stellen die Basis für nachfolgende Publikationsschritte dar. Sie bestehen aus (teil-)aggregierten Daten.

Zu den Produktdaten zählen auch die aggregierte Daten, welche für einen einzelnen oder mehrere Auftraggeber spezifisch aufbereitet wurden.

Produktdaten bestehen aus Fakttabellen (mit Referenzen zu den benötigten Dimensionen, d.h. Nomenklaturen, Wertebereiche etc.). Während die POEen in den Working Areas beliebige (meist toolbedingte) Cube-/Data Mart-Implementationen verwenden, werden Cubes im Datenbereich in einem festgelegten "Einheits-Format" gespeichert.

Physisches Format:
a) Data Marts: Das Darstellungs-Format im Data Pool wird festgelegt als Star Schema (oder Snowflake-Schema) auf relationaler Basis. Dieses Format ermöglicht es, anlässlich des Transfers vom Datenbereich in die betreffende WorkingArea oder umgekehrt die Daten in/von jedes/m andere/n benötigte/n Cube-Format offen und generisch umzuwandeln.
b) Tabellen werden als Relationale Tabellen gespeichert (d.h. als Tabellen innerhalb einer Datenbank).

Publikationsdaten
Dieser Datenbereich enthält drei unterschiedliche Datenarten:

1. Alle zur öffentlichen Verwendung freigegebenen Standard-Publikationen. Diese Daten müssen alle Anforderungen des Datenschutzes erfüllen.

   Publikationsdaten werden einerseits durch einen inhaltlichen Produktionsprozess und anschliessender redaktioneller Bearbeitung erstellt und stellen damit "grafische Erzeugnisse" dar; anderseits können Publikationsdaten auch (bearbeitete und/oder redigierte) Konsolidierte Daten, Produktdaten oder Metadaten sein, ggf. durch erklärende Texte begleitet (Register, Nomenklaturen usw.).

2. Alle an Dritte direkt gelieferten Daten (Individualisierte Artikel). Wie oben können solche Daten Konsolidierte Daten, Produktdaten oder Metadaten sein. Im Gegensatz zu den obigen Publikationsdaten sind diese jedoch nicht öffentlich, sondern nur den jeweiligen Partnern zugänglich.

3. In diesem Bereich werden auch die sog. Informationsobjekte gespeichert, da diese logisch ebenfalls zu den Publikationsdaten gehören, auch wenn sie ihrer Natur nach mit "Halbfabrikaten" zu vergleichen sind.

11.2 Anhang 2: Rechtliche Grundlagen

1. Bundesstatistikgesetz (BStatG; SR 431.01)

Art. 14*a Datenverknüpfungen*
1 Zur Erfüllung seiner statistischen Aufgaben kann das Bundesamt Daten miteinander verknüpfen, wenn diese anonymisiert werden. Werden besonders schützenswerte Daten verknüpft oder ergeben sich aus der Verknüpfung Persönlichkeitsprofile, so sind die verknüpften Daten nach Abschluss der statistischen Auswertungsarbeiten zu löschen. Der Bundesrat regelt die Einzelheiten.
2 Statistikstellen der Kantone und Gemeinden dürfen zur Erfüllung ihrer statistischen Aufgaben Daten des Bundesamtes nur mit dessen schriftlicher Zustimmung und unter Berücksichtigung seiner Auflagen mit weiteren Daten verknüpfen.

2. Registerharmonisierungsgesetz (RHG; SR 431.02)

Art. 16 *Verwendung der Daten für Zwecke der Statistik, Forschung und Planung durch das Bundesamt*
1 Die Daten dienen dem Bundesamt für statistische Erhebungen und Auswertungen.
2 Das Bundesamt kann auf der Grundlage der Daten Stichproben für statistische Erhebungen ziehen.
3 Es kann Daten nach Artikel 6 Buchstaben a–h, j, k und m als Adressverzeichnis für die Durchführung statistischer Erhebungen verwenden.
4 Es kann zur Erfüllung seiner statistischen Aufgaben die Daten ohne Personenbezeichnungen mit denjenigen des GWR und des Betriebs- und Unternehmensregisters (BUR) dauerhaft verknüpfen und aufbewahren.

3. Bundesgesetz über den Datenschutz (DSG; SR 235.1)

Art. 22 *Bearbeiten für Forschung, Planung und Statistik*
1 Bundesorgane dürfen Personendaten für nicht personenbezogene Zwecke, insbesondere für Forschung, Planung und Statistik bearbeiten, wenn:
a. die Daten anonymisiert werden, sobald es der Zweck des Bearbeitens erlaubt;
b. der Empfänger die Daten nur mit Zustimmung des Bundesorgans weitergibt;
und
c. die Ergebnisse so veröffentlicht werden, dass die betroffenen Personen nicht bestimmbar sind.
2 Die Anforderungen der folgenden Bestimmungen müssen nicht erfüllt sein:
a. Artikel 4 Absatz 3 über den Zweck des Bearbeitens
b. Artikel 17 Absatz 2 über die Rechtsgrundlagen für die Bearbeitung von besonders schützenswerten Personendaten und Persönlichkeitsprofilen;
c. Artikel 19 Absatz 1 über die Bekanntgabe von Personendaten.

4. Verordnung über die Durchführung von statistischen Erhebungen des Bundes (Statistikerhebungsverordnung; SR 431.012.1)

2*a*. Abschnitt: Datenverknüpfungen

Art. 13*h Begriff*
Als Datenverknüpfung gilt die Verbindung von Daten aus verschiedenen Datenquellen wie Erhebungen, Registern, Verwaltungsdaten und Messdaten.

Art. 13*i Grundsätze*
1 Datenverknüpfungen dienen der Beschaffung statistischer Informationen unter Vermeidung von Erhebungen.
2 Sie werden nur durchgeführt, soweit sie für statistische Arbeiten geeignet und notwendig sind.

Art. 13*j Voraussetzungen*
1 Daten werden nur verknüpft, wenn sie die für statistische Arbeiten erforderliche Eignung und Qualität aufweisen.
2 Zur Erfüllung seiner statistischen Aufgaben kann das BFS sowohl eigene Daten als auch Daten, über die es keine Datenherrschaft hat (Drittdaten), verknüpfen.
3 Wer dem BFS Drittdaten zur Verknüpfung im Auftrag liefert (Art. 13*k*), muss nachweisen, dass:
a. ihre Erhebung und Übermittlung an das BFS sowie ihre Verknüpfung rechtmässig sind; und
b. sie die statistisch erforderliche Qualität aufweisen.
4 Die Statistikstellen der Kantone und Gemeinden dürfen zur Erfüllung ihrer statistischen Aufgaben Daten des BFS untereinander sowie mit ihren eigenen Daten verknüpfen, wenn sie sich in einem Datenschutzvertrag dazu verpflichten:
a. den Datenschutz in gleichem Masse zu gewährleisten wie das BFS;

b. die Daten des BFS nicht ohne dessen schriftliche Zustimmung weiterzugeben;
c. ihre fachliche Unabhängigkeit von Vollzugsorganen zu gewährleisten;
d. ein Datenbearbeitungsreglement zu erlassen und umzusetzen;
e. hinreichende Massnahmen für die Datensicherheit und den Datenschutz zu treffen;
f. die Standards vorbildlicher Verfahren der Statistik einzuhalten.

Art. 13*k Verknüpfungen im Auftrag Dritter*
1 Verknüpfungen im Auftrag Dritter für nicht personenbezogene Zwecke wie Forschung, Planung und Statistik führt das BFS im Rahmen eines Datenschutzvertrags nach Massgabe seiner technischen, organisatorischen und personellen Möglichkeiten durch. Es unterstützt insbesondere Verknüpfungsprojekte von Bund und Kantonen.
2 Die Entschädigung richtet sich nach der Verordnung vom 25. Juni 2003[32] über die Gebühren und Entschädigungen für statistische Dienstleistungen von Verwaltungseinheiten des Bundes.
3 Im Interesse der Kosten- und Arbeitseffizienz kann das BFS den Auftraggeber für bestimmte Aufgaben in den Verknüpfungsprozess einbeziehen. Diese Aufgaben werden im Datenschutzvertrag klar umschrieben.

Art. 13*l Weitergabe verknüpfter Daten*
Soweit das Gesetz für nicht personenbezogene Zwecke wie Forschung, Planung und Statistik die Weitergabe von Daten an Forschungs- und Statistikstellen des Bundes sowie an Dritte vorsieht, kann das BFS verknüpfte Daten unter den Voraussetzungen nach Artikel 9 weitergeben.

Art. 13*m Vernichtung verknüpfter Daten*
1 Verknüpfte Daten sind nach Abschluss der statistischen Auswertungsarbeiten zu vernichten, wenn sie besonders schützenswerte Daten oder Persönlichkeitsprofile enthalten.
2 Die übrigen verknüpften Daten dürfen für statistische Arbeiten weiterverwendet werden.

Art. 13*n Kennzeichnung von Datenverknüpfungen*
Statistiken, für die systematisch Datenverknüpfungen durchgeführt werden, sind im Anhang als solche gekennzeichnet.

5. Verordnung des EDI über die Verknüpfung statistischer Daten (Datenverknüpfungsverordnung; SR 431.012.13)

vom 17. Dezember 2013 (Stand am 15. Januar 2014)
Das Eidgenössische Departement des Innern (EDI),
gestützt auf Artikel 14 der Statistikerhebungsverordnung vom 30. Juni 1993[1],
verordnet:

Art. 1 *Gegenstand*
1 Diese Verordnung regelt die Organisation, den Ablauf, den Datenschutz und die Datensicherheit bei der Verknüpfung statistischer Daten durch das Bundesamt für Statistik (BFS) sowie die Voraussetzungen und die Organisation des Einbezugs Dritter in den Verknüpfungsprozess.
2 Sie regelt zudem die Anforderungen an die beteiligten Statistikstellen der Kantone und Gemeinden.

Art. 2 *Organisation und Ablauf der Datenverknüpfung*
1 Die Durchführung von Datenverknüpfungen im BFS setzt ein schriftliches und begründetes Gesuch an die Direktion des BFS voraus.
2 Das Gesuch wird von den betroffenen Fachsektionen, vom Methodendienst und vom Rechtsdienst des BFS auf seine fachliche, methodische und rechtliche Durchführbarkeit und Gültigkeit überprüft.
3 Über die Zulässigkeit und die Durchführung von Datenverknüpfungen entscheidet die Direktion des BFS.
4 Für die Verwaltung und Herausgabe der zur Durchführung von Datenverknüpfungen erforderlichen Verbindungsschlüssel und für die Überwachung der Datenverknüpfungen ist der Direktionsstab zuständig.

Art. 3 *Datenschutz und Datensicherheit*
1 Die zur Durchführung von Datenverknüpfungen erforderlichen Verbindungschlüssel werden zentral und in besonders gesicherter Form aufbewahrt.
2 Die Benutzung eines Verbindungsschlüssels im Einzelfall setzt die schriftliche Erlaubnis der Direktion des BFS voraus.
3 Die Abgabe der Verbindungsschlüssel erfolgt durch den Direktionsstab an die zur Durchführung der Datenverknüpfung berechtigten Einzelpersonen. Sie wird protokolliert.
4 Das BFS stellt sicher, dass Datenverknüpfungen nach dem jeweils aktuellen Stand der Technik und unter Einhaltung vorbildlicher statistischer Verfahren durchgeführt werden.

Art. 4 *Einbezug Dritter in den Verknüpfungsprozess*
1 Die Form und der Inhalt der Mitwirkung Dritter an der Durchführung der Datenverknüpfung sowie die Nutzung der verknüpften Daten werden vorgängig in einem Datenschutzvertrag geregelt.
2 In den Verknüpfungsprozess einbezogene Dritte erledigen ihre Arbeiten an einem gesicherten Arbeitsplatz innerhalb des BFS, der weder Datenimporte noch Datenexporte zulässt.

3 Das BFS übergibt den Dritten die verknüpften Daten, nachdem es deren Form und Inhalt überprüft hat.

Art. 5 *Anforderungen an die beteiligten Statistikstellen der Kantone und Gemeinden*
Statistikstellen der Kantone und Gemeinden dürfen Verknüpfungen von Daten des BFS nur durchführen, wenn sie:
a. über das erforderliche statistische Knowhow verfügen, um Datenverknüpfungen inhaltlich und methodisch fachgerecht sowie in der erforderlichen Qualität durchzuführen;
b. ausschliesslich eine statistische Tätigkeit ausüben, die unabhängig ist von Aufsichts-, Vollzugs- oder Regulierungstätigkeiten;
c. die statistische Geheimhaltung und den Schutz von Personendaten gewährleisten; und
d. alle statistischen Arbeiten unter Wahrung der wissenschaftlichen Unabhängigkeit und Objektivität durchführen.

Art. 6 *Bearbeitungsreglement*
Das BFS erlässt ein Bearbeitungsreglement, das die weiteren Einzelheiten der Durchführung von Datenverknüpfungen regelt.

Art. 7 *Inkrafttreten*
Diese Verordnung tritt am 15. Januar 2014 in Kraft.

6. Verordnung zum Bundesgesetz über den Datenschutz (VDSG; SR 235.11)

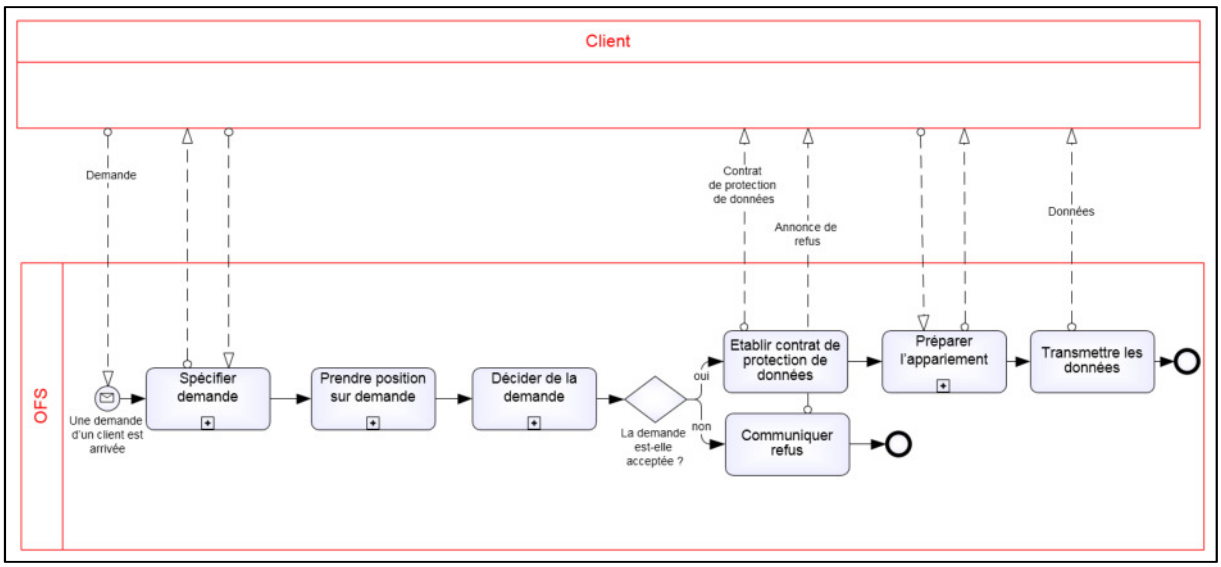
Art. 21 *Bearbeitungsreglement*
1 Die verantwortlichen Bundesorgane erstellen ein Bearbeitungsreglement für automatisierte Datensammlungen, die:
a. besonders schützenswerte Daten oder Persönlichkeitsprofile beinhalten;
b. durch mehrere Bundesorgane benutzt werden;
c. Kantonen, ausländischen Behörden, internationalen Organisationen oder privaten Personen zugänglich gemacht werden; oder
d. mit anderen Datensammlungen verknüpft sind.
2 Das verantwortliche Bundesorgan legt seine interne Organisation in dem Bearbeitungsreglement fest. Dieses umschreibt insbesondere die Datenbearbeitungs- und Kontrollverfahren und enthält alle Unterlagen über die Planung, Realisierung und den Betrieb der Datensammlung. Das Reglement enthält die für die Meldepflicht erforderlichen Angaben (Art. 16) sowie Angaben über:
a. das für den Datenschutz und die Datensicherheit der Daten verantwortliche Organ;
b. die Herkunft der Daten;
c. die Zwecke, für welche die Daten regelmässig bekannt gegeben werden;
d. die Kontrollverfahren und insbesondere die technischen und organisatorischen Massnahmen nach Artikel 20;
e. die Beschreibung der Datenfelder und die Organisationseinheiten, die darauf Zugriff haben;
f. Art und Umfang des Zugriffs der Benutzer der Datensammlung;
g. die Datenbearbeitungsverfahren, insbesondere die Verfahren bei der Berichtigung, Sperrung, Anonymisierung, Speicherung, Aufbewahrung, Archivierung oder Vernichtung der Daten;
h. die Konfiguration der Informatikmittel;
i. das Verfahren zur Ausübung des Auskunftsrechts.
3 Das Reglement wird regelmässig aktualisiert. Es wird den zuständigen Kontrollorganen in einer für diese verständlichen Form zur Verfügung gestellt.

11.3 Anhang 3: Bearbeitungsreglement (Template)

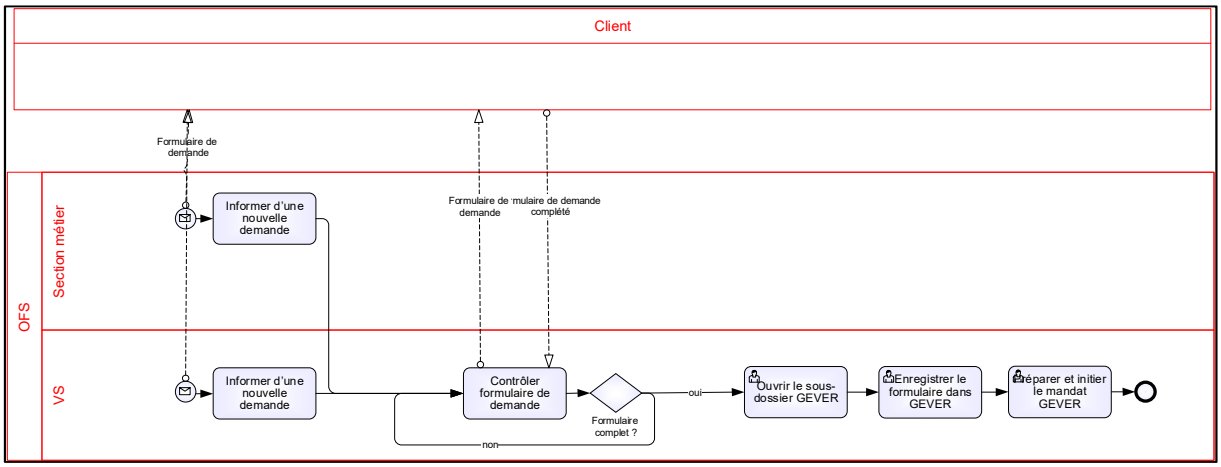
Das Template ist im elektronischen Archiv des BFS (nur intern zugänglich) abgelegt.
https://gever.edi.intra.admin.ch/edi/mx/COO.2080.104.5.652252?

11.4 Anhang 4: Prozessbeschreibungen (siehe auch Kap. 10)

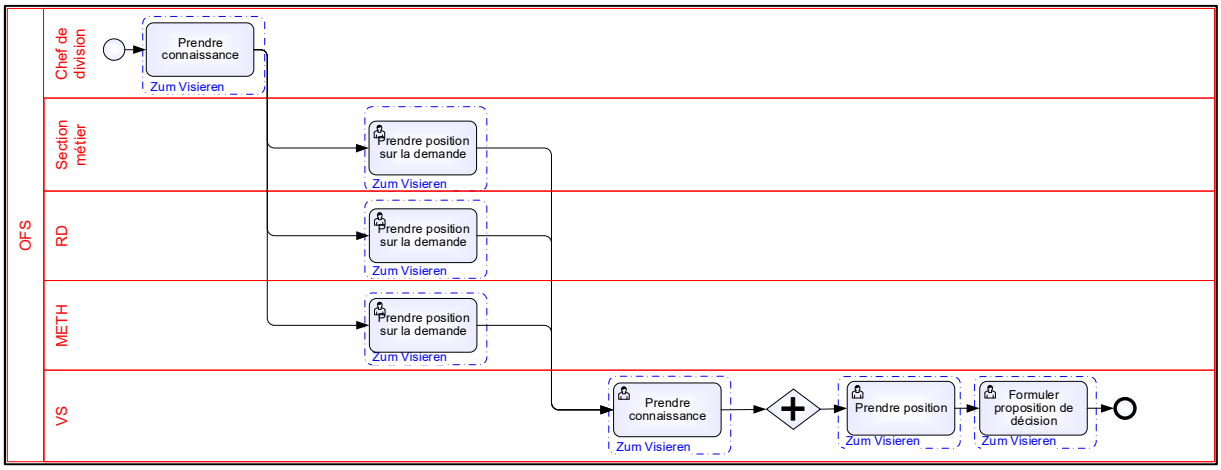
11.4.1 Traiter une demande d'appariement (vue d'ensemble)



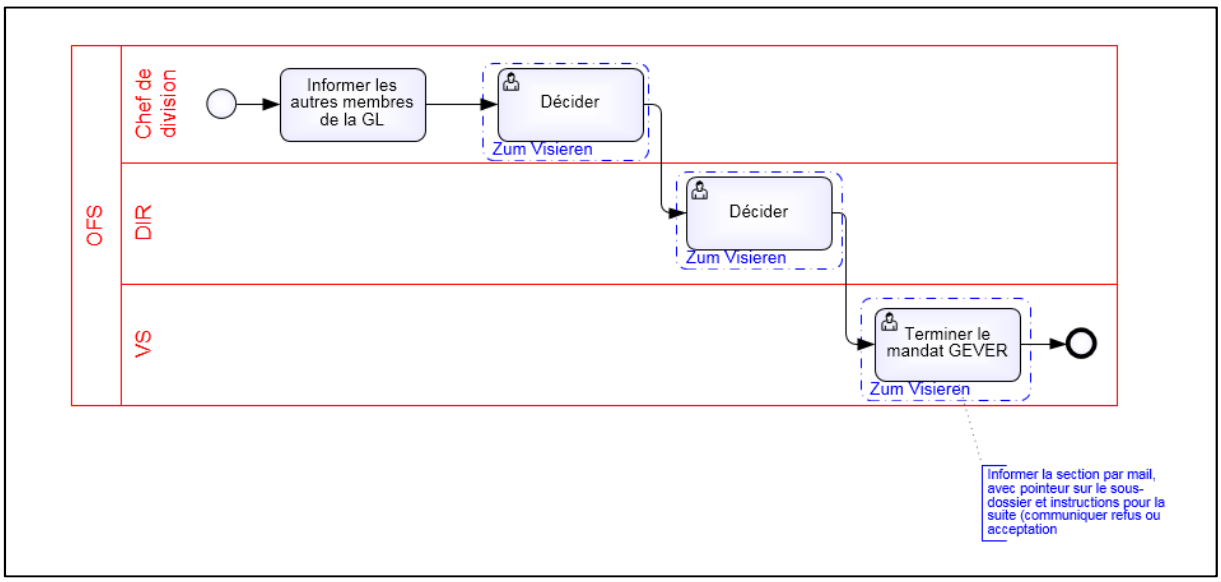
1. Spécifier la demande



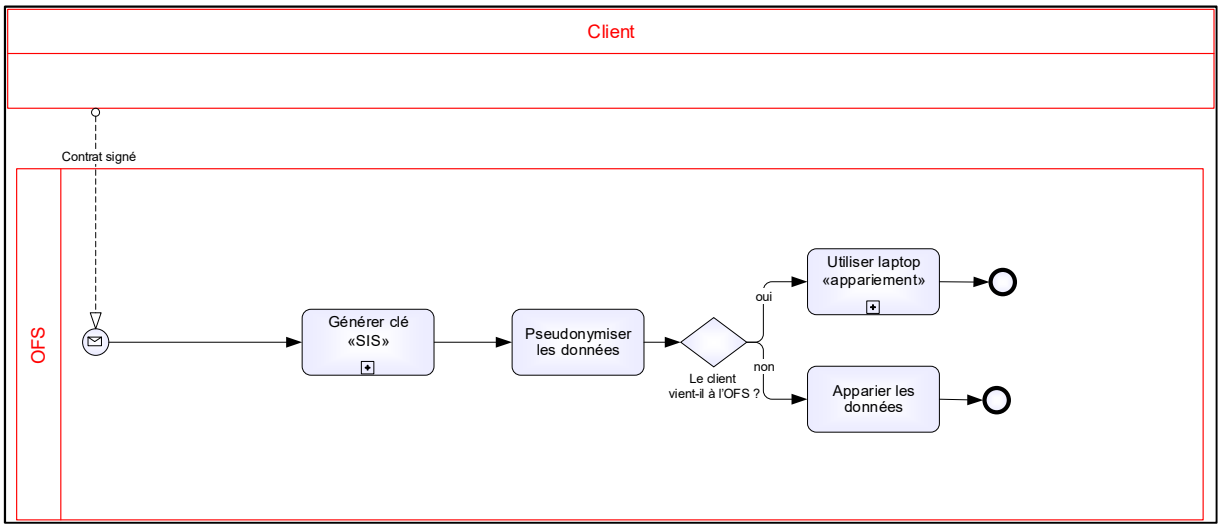
2. Prendre position sur la demande



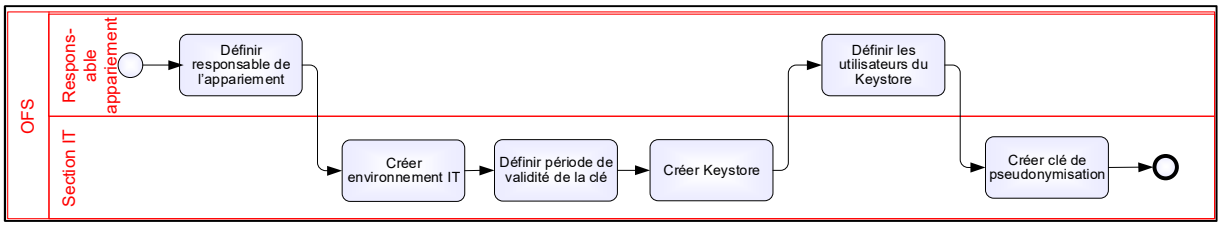
3. Décider de la demande



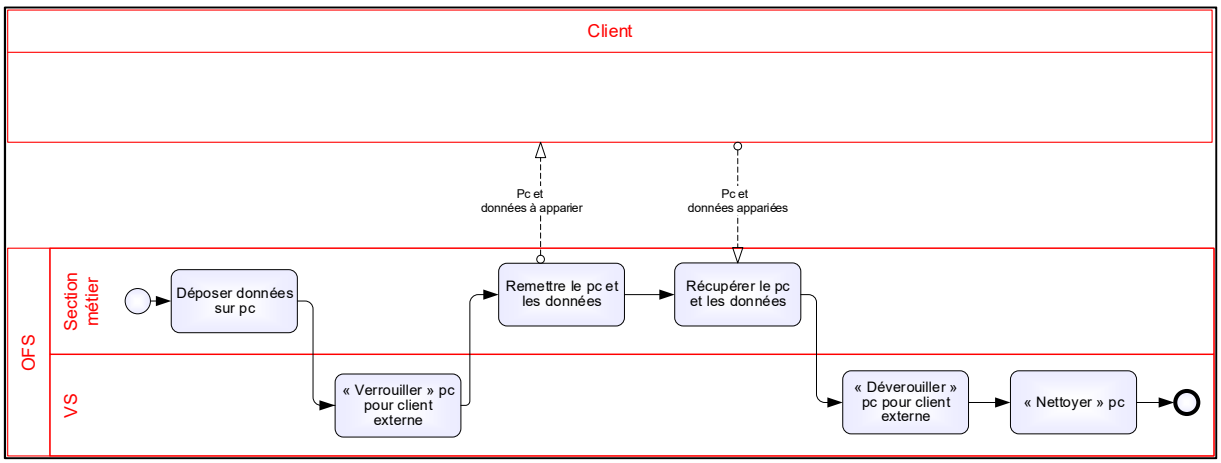
4. Préparer l‘appariement



4.1 Générer une clé de pseudonymisation „SIS



4.2 Utiliser un pc « appariement »



VS coordonne le verrouillage/déverrouillage qui est effectué par l'OSS du BIT.

Remarque : cette documentation des processus a été réalisée avec MS Visio. Le fichier original peut être consulté ici (uniquement interne à l'OFS) : Processus (214.0-00667/00001)

11.5 Anhang 5: Formulare

Antrag, Beurteilung und Entscheid:
https://www.bfs.admin.ch/bfs/de/home/dienstleistungen/datenverknuepfungen/fuer-dritte.assetdetail.7806087.html

11.6 Anhang 6: Datenaufbewahrung in Clouds

Im Rahmen eines Verknüpfungsvorhabens gelieferte Daten dürfen von Dritten nicht in einer Cloud gespeichert werden. Dies wurde in einem Austausch mit dem EDÖB entschieden und in einer Notiz festgehalten (nur BFS-Intern): Datenspeicherung_in_Cloud (053.0-1/00008)

Ein Kriterienkatalog wurde erarbeitet, um über Ausnahmen zu entscheiden (nur BFS-Intern): SpeicherungGeteilteUmgebung_D_final