



Marco D'Angelo, 01.06.2025

Directives de l'OFS sur l'appariement des données

Version:	Date:	Utilisation :
0.1	22.05.2015	Séance du groupe de travail du 22.05.2015 (titre «Note de discussion»)
0.2	08.06.2015	Séance du groupe de travail du 10.06.2015 (titre «Note de discussion»)
0.3	17.06.2015	Séance du groupe de travail du 23.06.2015 (titre «Note de discussion»)
0.9	24.06.2015	Séance de la GL du 22 janvier 01.07.2015 (titre «Note de discussion»)
0.91	22.09.2015	Première ébauche pour la séance du groupe de travail du 24.09.2015
0.93	24.09.2015	Ébauche pour la séance du groupe de travail du 24.09.2015
0.94	29.09.2015	Séance de la GL du 07.10.2015
0.95	29.09.2015	Séance de la GL du 07.10.2015 (version contenant les révisions)
0.96	27.10.2015	Version pour la séance du groupe de travail du 19.11.2015
0.97	19.11.2015	Version pour le colloque de l'OFS du 25.11.2015
1.1	08.11.2016	Version pour la séance du groupe de travail du 20.12.2016 (validée)
1.2	05.03.2020	Version contenant les adaptations des nouvelles conditions-cadres
1.3	02.06.2025	Version contenant les adaptations des nouvelles conditions-cadres

Glossaire

Abréviation	Signification
AC	Chef/fe de division de l'OFS
BUR	Registre des entreprises et des établissements,
COP	Code of Practice (code de bonnes pratiques)
DC	Données consolidées
DFI	Département fédéral de l'intérieur
DPS	Data Pseudonymisation Service
ESPA	Enquête sur la population active
FACH	Section métiers de l'OFS
GL	Conseil de direction de l'OFS (= Geschäftsleitung des BFS)
ISBO	Délégué à la sécurité informatique de l'unité organisationnelle
IT	Section Informatique de l'OFS
KMS	Keystore Management System
LHR	Loi fédérale sur l'harmonisation des registres des habitants et d'autres registres officiels de personnes
LSF	Loi sur la statistique fédérale
METH	Section Méthodes statistiques de l'OFS
OFIT	Office fédéral de l'informatique et de la télécommunication
OFS	Office fédéral de la statistique (OFS)
OLPD	Ordonnance relative à la loi fédérale sur la protection des données
OPDo	Ordonnance sur la protection des données
PFPDT	Préposé fédéral à la protection des données et à la transparence
PPA	Programme pluriannuel de l'OFS
RegBL	Registre des bâtiments et des logements.
SAS	Statistique de l'aide sociale
SC	Chef de section de l'OFS
SE	Relevé structurel
SESAM	Syntheseerhebung Soziale Sicherheit und Arbeitsmarkt
SILC	Enquête sur les revenus et les conditions de vie (SILC)
SIS	Statistical Information System
SJ	Service juridique de l'OFS
SMS	Statistical Metadata System
STATENT	Statistique structurelle des entreprises
STATPOP	Statistique de la population et des ménages
SUS	Statistique des condamnations pénales
VS	Service d'appariement de l'OFS (Verknüpfungsstelle des BFS)

Table des matières

1	Résumé	5
2	Contexte	5
3	Buts des directives	7
3.1	D'une approche axée sur les enquêtes à une approche axée sur les résultats	7
3.2	Protection et sécurité des données	7
4	Lien avec le programme pluriannuel de la statistique fédérale et les buts de l'office, des divisions et des sections	8
5	Cadre légal	8
6	Bases de l'appariement	9
6.1	Définitions	9
6.1.1	Qu'est-ce qu'un appariement?	9
6.1.2	Catégories d'appariements	10
6.2	Principes applicables	13
6.3	Prescriptions relatives à l'appariement	14
6.4	Sensibilité des données	18
7	Production statistique, sécurité et appariement des données	20
7.1	Processus de production statistique	20
7.2	Protection des données	21
7.2.1	Espace de confiance de l'OFS	21
7.2.2	Secteurs – Droits d'accès aux données	22
7.2.3	Pseudonymisation des données consolidées – droits d'accès aux clés	22
7.3	Pseudonymisation, dépseudonymisation et repseudonymisation	22
7.4	Principe de la gestion des clés de pseudonymisation	24
8	Organisation et rôles	24
9	Éléments de l'appariement de données	26
9.1	Inventaires des appariements à l'OFS	26
9.2	Demandes d'appariement	27
9.3	Règlement de traitement	28
9.4	Association de tiers aux travaux d'appariement	28
9.5	Appariements par les services de statistique régionaux	28
10	Processus d'appariement	29
10.1	Remarques préliminaires	29
10.2	Vérification de la demande et prise de décision	29
10.2.1	Vérification de la demande	29
10.2.2	Décision	30
10.3	Réalisation de l'appariement	31
10.3.1	Étapes de l'appariement	31
10.3.2	Appariement par des services cantonaux ou communaux	32
10.4	Remise de données appariées	32
10.5	Clôture du projet d'appariement et effacement des données appariées	32
11	Annexes	34

Directives sur l'appariement

11.1	Annexe 1: Définitions (concept SIS)	34
11.2	Annexe 2: Bases légales	36
11.3	Annexe 3: Description des processus (voir aussi chapitre 10)	40
11.3.1	Traitement de la demande (vue globale)	40
11.3.2	Précision de la demande	40
11.3.3	Prise de position	41
11.3.4	Décision	41
11.3.5	Réalisation de l'appariement.....	42
11.3.6	Création clé SIS	42
11.4	Annexe 4: Formulaires	43
11.5	Annexe 5: Conservation des données sur le nuage	43

1 Résumé

L'appariement de données vise à produire des informations nouvelles à partir des données existantes et de les valoriser, tout en évitant des relevés superflus, en allégeant la charge des personnes interrogées, en créant des synergies et en établissant des sources d'informations élargies. Il consiste à relier entre elles des données individuelles qui proviennent de différentes sources, en créant une nouvelle base de données devant permettre l'accomplissement de tâches statistiques. On distingue trois types d'appariement de données, à savoir (i) les appariements destinés à la production statistique, (ii) les appariements longitudinaux et (iii) les appariements destinés à l'analyse. Dans un souci de traçabilité, les projets d'appariement sont répertoriés dans un inventaire.

Les appariements effectués à l'OFS satisfont à des conditions très strictes de protection et de sécurité des données. Les appariements destinés à la production de statistiques et à l'analyse doivent être approuvés par le responsable du domaine Production statistique dans le cadre d'un processus de demande, les appariements longitudinaux par le service d'appariement. Les données à appairer sont pseudonymisées à l'aide d'une clé spécifique au projet. Les personnes responsables au sein des sections métier gèrent les droits d'accès à ces clés de pseudonymisation.

Deux organes ont été constitués pour encadrer les projets d'appariement: le service d'appariement, qui coordonne les travaux administratifs dans le cadre de la procédure d'évaluation et qui gère les clés en collaboration avec le service informatique, et le groupe de travail Appariements.

Aussi bien les sections de l'OFS que des instances externes peuvent soumettre des demandes d'appariements. L'OFS se charge généralement des appariements comme énoncés à l'art. 14a, al. 1, LSF, mais les services régionaux de statistiques peuvent également s'en charger sous certaines conditions.

2 Contexte

Les travaux sur l'appariement de données menés depuis 2010¹ ont débouché sur une structure en trois volets:

- Orientation générale
- Bases légales
- Organisation/processus/informatique

En 2014, un règlement de traitement a été présenté (règlement de traitement «Appariements», état au 13 octobre 2014). Soumis au Préposé fédéral à la protection des données et à la transparence (PFPDT), il a reçu un avis favorable. Les travaux n'étaient cependant pas terminés. Lors de la réunion d'avril 2015, l'état d'avancement des travaux a été présenté au conseil de direction (GL) de l'OFS; sur cette base, la GL a établi un état des lieux et formulé des questions. En juillet 2015, le conseil de direction s'est penché sur une note de discussion basée sur le règlement de traitement de 2014. Ce dernier a été révisé, puis approuvé par le conseil de direction en décembre 2015.

En 2018, le PFPDT a effectué une visite à l'OFS lors de laquelle la procédure à suivre en matière d'appariement de données lui a été présentée. Le PFPDT a pris connaissance de la documentation établie par l'OFS.

Le message a également été transmis aux organes Fedestat et Corstat dans le cadre de visites à l'OFS, à savoir que des appariements sont intégrés dans le système statistique public de la Suisse.

¹ Note de discussion 2010, version 1.0 du 25 août 2010

Directives sur l'appariement

Le présent document résume les informations pertinentes concernant les appariements de données à l'OFS et règle les processus concrets visant à garantir la protection et la sécurité des données. Il est régulièrement mis à jour.

Un appariement se fait en deux étapes:

- la pseudonymisation spécifique au projet
- La liaison (join) de jeux de données

Ce dernier point est généralement accompli par le dépositaire de la demande.

3 Buts des directives

3.1 D'une approche axée sur les enquêtes à une approche axée sur les résultats

La plupart des statistiques étaient autrefois fondées sur des relevés: chaque statistique faisait l'objet d'un relevé spécifique. La production statistique a été adaptée de manière à gagner en efficacité, dans le but d'éviter les doublons, de décharger les personnes interrogées et de mieux exploiter les synergies. Conformément à l'art. 4 LSF, les données statistiques doivent être obtenues en premier lieu sans réaliser de relevés directs (enquêtes), autrement dit en recourant de manière systématique à des registres et à des données administratives. Cela passe par des systèmes d'informations intégrés, qui sont axés sur l'output et qui se fondent sur des relevés coordonnés de données provenant de différentes sources (registres, données administratives ou enquêtes). Les données sont appariées (reliées entre elles) et exploitées pour produire l'output souhaité (statistiques). En plus de favoriser la réutilisation des données, un tel système a comme avantage de permettre la réalisation de nouvelles statistiques à partir des données disponibles. Les besoins croissants en informations des milieux économiques et politiques, de la société, de l'administration et de la recherche s'en trouvent ainsi mieux satisfaits. Ce système permet en outre de tenir compte du principe *once only*² qu'applique l'administration fédérale.

3.2 Protection et sécurité des données

La [loi sur la statistique fédérale \(LSF, RS 431.01\)](#)³, l'ordonnance sur la statistique fédérale (OStatF, RS 431.011), la [loi sur la protection des données](#) (LPD, RS 235.1), l'ordonnance sur la protection des données (OPDo, RS 235.11), le [code de bonnes pratiques d'Eurostat](#), la [Charte de la statistique publique de la Suisse](#) et [l'ordonnance sur la sécurité de l'information \(OSI\)](#) s'appliquent au sein de l'office. L'office applique les mesures suivantes pour garantir la protection et la sécurité des données:

- Authentification forte (accès au moyen de la Smartcard)
- Accès limité: seules les personnes habilitées peuvent accéder aux données
- Signature par chaque membre du personnel d'une déclaration par laquelle il accepte de se conformer aux règles de protection des données
- Communication de données individuelles pseudonymisées
- Conclusion d'un contrat de protection des données avec les utilisateurs externes

D'autres mesures sont nécessaires pour garantir notamment la transparence des appariements et des processus, la protection des données et la pseudonymisation des données individuelles.

Les éléments suivants doivent être réglementés afin de satisfaire aux exigences et de garantir que l'appariement se fasse de manière contrôlée, sûre et transparente:

- les définitions (chapitre 6.1)
- les principes régissant l'appariement (chapitre 6.2)
- les conditions de l'appariement (chapitre 6.3)
- les dispositions techniques et la gestion des données (chapitre 0)
- l'organisation, les rôles et les compétences (chapitre 8)
- les processus d'appariement (chapitre 10)

² [Décision du Conseil fédéral du 27 septembre 2019, Stratégie Administration fédérale numérique](#),

³ Les lois sont disponibles sur la page suivante, en indiquant leur numéro RS: [Recueil systématique des lois | Fedlex](#)

4 Lien avec le programme pluriannuel de la statistique fédérale et les buts de l'office, des divisions et des sections

L'objectif 2 «Mettre à profit le potentiel de l'utilisation multiple des données ainsi que celui de nouvelles méthodes de relevé et d'analyse pour une production statistique ciblée, automatisée et efficace» du [Programme pluriannuel PPA 2024 – 2027](#) met l'accent sur l'appariement des données. Ce point figure dans le PPA depuis 2015.

Les objectifs de l'OFS intègrent l'objectif susmentionné du programme pluriannuel. Le groupe de travail Appariements remplit l'objectif suivant: exploiter le potentiel de l'appariement des données selon les processus et les structures définis et optimiser constamment ce potentiel par le recours aux bonnes pratiques et les échanges avec les divisions.

5 Cadre légal

Les bases légales en vigueur, à savoir l'art. 14a LSF, l'art. 16 al. 4 LHR ([loi sur l'harmonisation des registres, RS 431.02](#)), l'art. 6 LPD, les art. 28 ss OStatF, Ordonnance du DFI concernant l'appariement de données statistiques (RS 431.012.13) et les présentes directives sur l'appariement des données fixent le cadre légal suivant:

Raison d'être: Les relevés directs sont fastidieux pour les personnes interrogées et suscitent parfois chez ces dernières du mécontentement et de l'incompréhension vis-à-vis de la Confédération (et plus particulièrement de l'OFS); les taux de réponses en souffrent, et la qualité des statistiques s'en trouve affectée à son tour. Pour pallier ce problème, l'art. 4, al. 3, LSF dispose que le nombre des enquêtes doit être limité au strict nécessaire. L'appariement de données doit permettre à l'OFS de préserver la qualité et la représentativité de ses statistiques.

Compétence: Au niveau fédéral, seul l'OFS est habilité à effectuer des appariements, afin de remplir ses tâches statistiques. Il s'agit d'une habilitation d'ordre général (art. 14a LSF). L'art. 16, al. 4, LHR autorise par ailleurs l'appariement de données des registres des habitants avec des données du RegBL et du REE.

Les services statistiques cantonaux et communaux peuvent appairer des données de l'OFS pour remplir leurs tâches statistiques à condition qu'ils aient l'autorisation de l'OFS et qu'ils satisfont à ses exigences.

D'autres tiers (demandeurs) peuvent être associés au processus d'appariement pour réduire les coûts et le travail engendrés. Ce sont généralement les tiers participant au processus d'appariement (art. 3, al. 2 de l'ordonnance sur l'appariement de données) qui s'occupent de lier les jeux de données à l'aide du pseudo-identificateur spécifique au projet. S'il y a lieu, les modalités doivent être stipulées de manière claire dans le contrat sur la protection des données.

Transparence: Une demande écrite et motivée doit être présentée pour chaque appariement. Dans le cas des appariements destinés à la production statistique et à l'analyse, la demande doit être soumise aux sections de production concernées, à la section Méthodes statistiques et au service juridique, qui en vérifient la faisabilité sur les plans technique, méthodologique et juridique. Dans le cas des appariements longitudinaux, la demande est généralement examinée directement par le service d'appariement.

Protection des données: Les appariements de données ne sont autorisés que s'ils sont nécessaires et adaptés aux travaux statistiques et qu'ils présentent la qualité requise à cet effet. Font exception les appariements test internes auxquels des critères spécifiques sont appliqués et qui servent à tester la qualité des données. Le service d'appariement doit conserver de manière sûre les clés nécessaires à la réalisation des appariements, conformément aux principes de gestion des clés. Les appariements doivent obligatoirement être réalisés avec les moyens informatiques et selon les processus de l'OFS. L'utilisation d'une clé doit être consignée par écrit pour chaque cas.

Les droits d'accès aux différentes données (données d'entrée, données consolidées et données de produits; voir chapitre 7.1 et annexe 1) doivent être réglés de manière claire et restrictive. Les données de différents projets doivent être pseudonymisées à l'aide d'une clé spécifique à chaque

Directives sur l'appariement

projet.

Les dispositions en vigueur imposent une documentation détaillée de tous les appariements afin de respecter le principe de transparence. Ces informations concernant les appariements sont contenues dans les fiches signalétiques, dans les règlements de traitement ou dans le formulaire de demande ainsi que dans la décision (du responsable du domaine Production statistique ou du service d'appariement) et sont classées dans les archives électroniques de l'OFS.

Les données appariées peuvent être remises à des tiers aux conditions fixées à l'art. 31 OStatF, pour autant qu'elles soient destinées à des fins non personnelles (recherche, planification, statistique, etc.), comme le prévoit la loi. La remise à des tiers dépend du degré de sensibilité des données, du but de leur utilisation et du demandeur. L'OFS n'a pas d'obligation de communiquer des données à des tiers. Les services cantonaux et communaux de statistique se doivent de garantir la protection des données, la sécurité des données et le secret statistique dans la même mesure que l'OFS, sans quoi ce dernier ne peut pas accepter qu'ils procèdent à des appariements.

L'annexe 2 contient les textes légaux pertinents.

6 Bases de l'appariement

6.1 Définitions

6.1.1 Qu'est-ce qu'un appariement?

L'OFS applique la définition suivante: un appariement de données consiste à relier des **données individuelles** provenant de **diverses sources** (art. 28 OStatF) afin de produire un nouveau **jeu de données**. Chaque nouvelle exploitation d'un registre ou nouvelle réalisation d'une enquête en fait une nouvelle source de données⁴. Pour qu'il s'agisse d'un appariement au sens de la statistique publique, il faut qu'il s'agisse d'un projet de recherche ou d'innovation d'importance nationale ou qu'il existe un lien étroit avec la statistique fédérale.

La distinction est faite entre les catégories d'appariement suivantes (voir aussi le chapitre 6.1.2 Catégories d'appariement):

- Appariements destinés à la production statistique
- Appariements longitudinaux
- Appariements destinés à l'analyse statistique

Les cas suivants ne constituent pas des appariements (et il n'existe pas d'autre exception):

- Séries chronologiques de données agrégées (p. ex. indices de prix, évolution de la production et de l'emploi, enquête sur la population active, etc.). Il ne s'agit pas de données individuelles (voir aussi le ch. 6.1.2 → point 2 de la page 9)
- Combinaison de données avec des nomenclatures ou ajout de géocoordonnées à l'aide d'adresses. Ces opérations servent uniquement à caractériser ou à structurer des informations.
- Regroupement de données de différentes sources dans le REE et dans le RegBL, tel que prévu dans les ordonnances respectives. Toute combinaison de données sortant de ce cadre est soumise aux prescriptions en matière d'appariement énoncées dans l'ordonnance sur les relevés statistiques, l'ordonnance du DFI sur l'appariement de données et le règlement de traitement s'y rapportant.
- Les enquêtes par panel, dans lesquelles les personnes répondent aux mêmes questions à différents intervalles. Ces enquêtes sont conçues au départ pour une réutilisation de l'échantillon et des réponses données lors de la précédente interview. Cette caractéristique

⁴ On peut citer comme exemple les appariements longitudinaux.

Directives sur l'appariement

est mentionnée dans l'ordonnance sur la statistique fédérale. On a ici affaire à une seule source de données⁵.

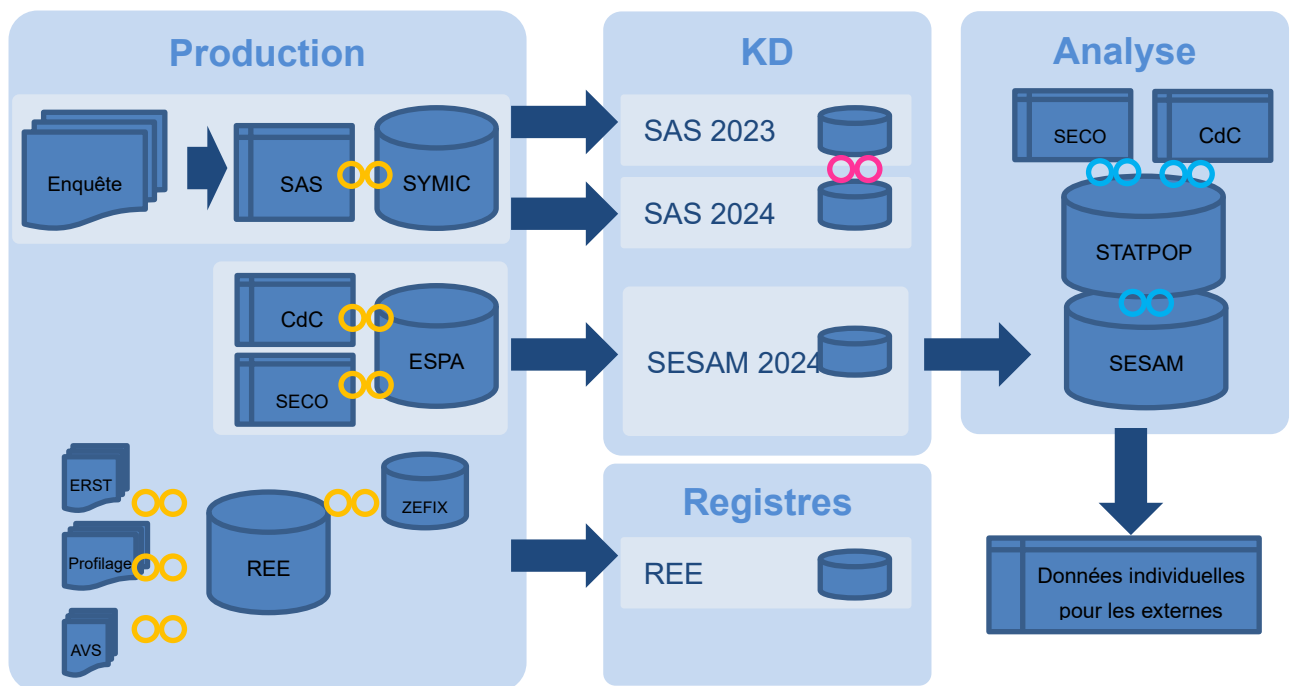
- Comparaison avec des données obtenues les années précédentes sur la base de la même enquête aux fins de plausibiliser les données et d'en vérifier la qualité.
- Comparaisons avec des sources de données uniquement aux fins d'assurer la qualité, de traiter les données au sens large, y compris de développer et d'améliorer les méthodes statistiques, dans le cadre de la production.

6.1.2 Catégories d'appariements

Pour garantir une bonne acceptation des appariements et une pratique homogène en la matière, l'OFS a opté pour une structure d'appariement aujourd'hui bien établie parmi ses collaborateurs et les spécialistes de la statistique: le *processus de valorisation de la production statistique* (voir aussi le chapitre 7.1). Il faut justifier chaque appariement et indiquer sa base légale. La plupart des activités statistiques sont énumérées dans l'*ordonnance sur la statistique fédérale*.

À partir de ce qui précède, on peut répartir les appariements en trois catégories:

1. Appariements destinés à la production statistique
2. Appariements longitudinaux
3. Appariements destinés à l'analyse statistique



1. Appariements destinés à la production statistique

L'OFS peut procéder à des appariements pour la production statistique dans le but d'établir des données consolidées en vertu de l'art. 29, al. 1 et 2, OStatF. La base légale pour ces appariements existe donc. Peu importe qu'un relevé de données (primaires) ait été au préalable réalisé ou non à l'OFS.

⁵ À l'inverse, la combinaison de données de l'ESPA et de la SILC avec des données de STATPOP et du REE sont considérées comme des appariements au sens des présentes directives.

Directives sur l'appariement

Conformément à l'art. 28, al. 2, let. a OStatF, ne sont pas considérés comme des appariements les comparaisons avec des sources de données uniquement aux fins d'assurer la qualité, de traiter les données au sens large, y compris de développer et d'améliorer les méthodes statistiques, dans le cadre de la production.

Enrichissement de répertoires et de registres

Un processus particulier de la production statistique consiste à appairer des registres et des répertoires afin d'en enrichir le contenu. Ces recueils constituent eux aussi des sources de données administratives. De tels regroupements de données (REE, STATENT, RegBL, etc.) représentent aussi des appariements et peuvent figurer dans l'ordonnance sur la statistique fédérale. Ces appariements présentent la particularité d'avoir leur propre base légale, tandis que les registres qu'ils alimentent sortent du cadre de valorisation statistique «classique».

Caractéristiques des appariements destinés à la production statistique

- Ils sont internes à l'OFS.
- Ils sont destinés à des tests et à la production.
- Ils nécessitent une seule autorisation; l'autorisation doit être renouvelée si des modifications sont apportées.
- Ils s'inscrivent dans l'inventaire de l'OFS.

Enrichissement de répertoires et de registres

- Ils reposent sur l'ordonnance propre aux registres.
- Les sources qui sont reliées aux répertoires et aux registres sont clairement indiquées.

2. Appariements longitudinaux

Les appariements longitudinaux consistent à associer les variables d'une même unité présentes dans des enquêtes ou des sources de données administratives identiques, mais réalisées à des moments différents (p.ex. à un rythme annuel ou pluriannuel), afin d'identifier des changements et des évolutions. Les appariements concernent uniquement des données individuelles et n'ont pas d'effet sur les séries temporelles obtenues à partir de données agrégées (p. ex. indices de prix, évolution de la production et de l'emploi, taux de chômage, etc.).

Exemples positifs d'appariements longitudinaux:

- 1) Combinaison de données individuelles tirées de relevés réalisés à des moments différents pour représenter une évolution (exemple: démographie des entreprises).
- 2) Établissement de parcours de formation individuels par la combinaison d'informations tirées de relevés qui se rapportent à des périodes différentes.

Exemples négatifs d'appariements longitudinaux:

- 1) Comparaison avec des données individuelles de l'année précédente aux fins de contrôle des réponses et de la qualité (exemples: statistique de la valeur ajoutée, statistique des caisses de pensions).
- 2) Enquêtes par panel, dans lesquelles les personnes répondent aux mêmes questions à différents intervalles (exemples: SILC, ESPA). Ces enquêtes sont conçues au départ pour une réutilisation de l'échantillon et des réponses données lors de la précédente interview. Cette caractéristique est mentionnée dans l'ordonnance sur la statistique fédérale.

Les appariements longitudinaux sont effectués par l'OFS à l'interne. Ils consistent normalement à relier les données consolidées d'une même enquête correspondant à différentes unités temporelles. Le résultat de cet appariement peut être considéré comme un produit figurant dans l'inventaire de l'OFS. Les utilisateurs externes qui souhaitent recourir à de telles données consolidées sur plusieurs unités temporelles peuvent le faire moyennant la conclusion d'un contrat de protection des données standard. Il en va de même lorsque la livraison des données n'englobe pas toutes les variables du produit.

Pour accomplir les tâches légales qui sont de son ressort, l'OFS peut procéder, sans déposer de

Directives sur l'appariement

demande, à des appariements de données à partir d'une même source, mais à des moments différents, en tenant compte des exigences fixées aux art. 29 à 33 OStatF.

Caractéristiques des appariements longitudinaux

- Ils sont destinés en premier lieu à l'analyse.
- Ils constituent généralement des «produits standardisés».
- Ils s'inscrivent dans l'inventaire de l'OFS.

Les externes peuvent obtenir les appariements longitudinaux qui existent déjà en signant un contrat relatif à la protection des données.

3. Appariements destinés à l'analyse statistique

Les appariements destinés à l'analyse statistique que l'OFS effectue en vertu de l'art. 14a LSF pour remplir ses tâches statistiques doivent avoir fait l'objet d'une demande documentée pour des raisons de légalité et de transparence. Cette règle vaut aussi bien pour les demandes internes que pour les demandes externes. Ces appariements ne servent pas à la production, mais à l'analyse de données (parcours de formation, projet NCCR de l'Université de Genève, p. ex.).

Caractéristiques des appariements destinés à l'analyse statistique

- Ils sont utilisés à des fins internes ou externes.
- Ils sont à caractère analytique.
- Ils sont généralement à usage unique.
- Les demandes sont fondées sur le processus décrit au chapitre 10 et dans l'annexe 5.
- Ils s'inscrivent dans l'inventaire de l'OFS.

Directives sur l'appariement

6.2 Principes applicables

L'appariement des données à l'OFS se fonde sur les principes suivants:

- L'OFS soutient et met en œuvre de manière ciblée l'appariement des données pour obtenir des informations statistiques de manière efficiente. L'appariement soutient l'utilisation multiple des données (*once-only*) et la minimisation des données (Administration numérique suisse).
- Les appariements sont exclusivement effectués à des fins statistiques au sens de la LSF; ils doivent être pertinents et proportionnels. Le besoin d'information doit être avéré; les appariements ne sont pas faits en réserve.
- Les appariements sont effectués en toute transparence et sont documentés. La base légale est vérifiée, les appariements sont inventoriés et validés.
- Les appariements doivent se justifier et être effectués selon une méthode correcte. Les données d'entrée comme les données de sortie doivent satisfaire aux exigences de qualité statistique usuelles. L'OFS ne censure toutefois pas les projets de recherche, car la liberté de recherche n'est pas remise en question.
- Les processus d'appariement sont soumis à des conditions strictes en matière de protection et de sécurité des données. Ils sont réalisés avec les outils prévus à cet effet et sont documentés.
- Leurs différentes étapes doivent être conçues aussi simplement que possible. Les complications inutiles et les obstacles administratifs sont à éviter dans la mesure du possible.
- Les étapes des processus représentés dans ces directives (voir chapitre 6.3 Prescriptions relatives aux appariements, chapitre 10 Processus d'appariement et annexe 4: Description des processus) s'appliquent à tous les demandeurs (internes et externes).
- Les appariements de données au sens de l'art. 14a LSF sont effectués principalement par l'OFS. L'OFS pseudonymise les données à l'aide d'une clé spécifique au projet. C'est généralement le demandeur qui s'occupe de mettre en relation les différents jeux de données.
- L'OFS vérifie les conditions légales (p. ex.: existe-t-il des bases légales pour le projet en question et le projet les respecte-t-il?) ainsi que la faisabilité du projet quant au contenu, à la méthodologie et sur le plan technique, dans les meilleurs délais et sous réserve de ressources suffisantes.
- La transmission de données appariées est possible dans le cadre de la réglementation applicable à la transmission de données individuelles (art. 31 OStatF). Elle dépend du degré de sensibilité des données, du but de leur utilisation et du demandeur. Un contrat de protection des données doit être conclu dans tous les cas.
- Les dispositions applicables comprennent, outre les règles concernant les appariements exposées dans le présent document, les prescriptions définies dans d'autres guides de l'OFS au sujet du traitement et de la remise de données individuelles ainsi que de la protection et de la sécurité des données⁶.
- Le coût des appariements est calculé d'après les barèmes de l'ordonnance sur les émoluments et indemnités perçus pour les prestations de services statistiques des unités administratives de la Confédération⁷.

⁶ Directives relatives à la protection des données en cas de transmission de données individuelles à des tiers, 18 octobre 2006 – révision nécessaire en attente

⁷ Cette ordonnance est en cours de révision et devrait entrer en vigueur le 15 juillet 2026.

Directives sur l'appariement

6.3 Prescriptions relatives à l'appariement

Catégories et conditions de l'appariement: Interne

	Conditions à remplir			
Catégorie d'appariement	Avant	Déroulement (voir aussi chap. 10.3.1)	Après	Réserves/ facilitations
1) Appariement destiné à la production statistique	• Demande par formulaire • Prise de position sections, METH et RD • Approbation par chef/fe de division, information aux autres membres de la GL • Décision du responsable du domaine thématique Production statistique • Création d'une clé de pseudonymisation spécifique au projet par le responsable de pseudonymisation⁸ • Inscription dans l'inventaire • Adaptation de la fiche signalétique	• Attribution de l'autorisation d'utiliser la clé aux data consumers compétents • Pseudonymisation/appariement spécifique à chaque cas	• Fin de validité de l'autorisation à utiliser la clé de pseudonymisation	• Mesures de sécurité supplémentaires ou limitations en cas d'appariement de données sensibles • Pas d'effacement de jeu de données appariées

⁸ Les rôles du responsable de pseudonymisation, de l'utilisateur de données, et d'autres sont définis au chapitre 8.

Directives sur l'appariement

	Conditions à remplir			
Catégorie d'appariement	Avant	Déroulement (voir aussi chap. 10.3.1)	Après	Réserves/facilitations
2) Appariements longitudinaux	• Demande par formulaire • Décision du service d'appariement • Création d'une clé de pseudonymisation spécifique au projet par le responsable de pseudonymisation Inscription dans l'inventaire	• Attribution de l'autorisation d'utiliser la clé aux data consumers compétents • Pseudonymisation/appariement spécifique à chaque cas	• Fin de validité de l'autorisation à utiliser la clé de pseudonymisation	• Pas d'effacement du jeu de données apparié • Mesures de sécurité supplémentaires ou limitations en cas d'appariement de données sensibles
3) Appariements destinés à l'analyse statistique	• Demande par formulaire • Prise de position sections, METH et RD • Approbation par chef/fe de division, information aux autres membres de la GL • Décision du responsable du domaine thématique Production statistique • Création d'une clé de pseudonymisation spécifique au projet par le responsable de pseudonymisation Inscription dans l'inventaire	• Attribution de l'autorisation d'utiliser la clé aux data consumers compétents • Pseudonymisation/appariement spécifique à chaque cas	• Fin de validité de l'autorisation à utiliser la clé de pseudonymisation	• Possibilité de simplifier la procédure pour les données non sensibles • Mesures de sécurité supplémentaires ou limitations en cas d'appariement de données sensibles • Effacement des appariements de données sensibles une fois l'analyse terminée

Directives sur l'appariement

Catégories et conditions de l'appariement: domaine externe

	Conditions requises			
Catégorie d'appariement	Avant	Exécution	Après	Réserves/ facilitations
1) Appariement destiné à la production statistique	-	-	-	-
2) Appariements longitudinaux	• Demande par formulaire • Décision du service d'appariement • Création d'une clé de pseudonymisation spécifique au projet par le responsable de pseudonymisation - Établissement d'un contrat de protection des données de type V • Inscription dans l'inventaire	• Attribution de l'autorisation d'utiliser la clé aux data consumers compétents • Pseudonymisation/appariement spécifique à chaque cas • Examen éventuel des données d'output par l'OFS	• Fin de validité de l'autorisation à utiliser la clé de pseudonymisation • Confirmation de la destruction des données	• Possibilité de simplifier la procédure pour les données non sensibles • Mesures de sécurité supplémentaires ou limitations dans la remise ou l'utilisation de données sensibles • Des tiers peuvent être associés à l'appariement, si nécessaire.

Directives sur l'appariement

	Conditions requises			
Catégorie d'appariement	Avant	Exécution	Après	Réserves/ facilitations
3) Appariements destinés à l'analyse statistique	• Demande par formulaire • Prise de position sections, METH et RD • Approbation par chef/fe de division, information aux autres membres de la GL • Décision du responsable du domaine thématique Production statistique • Création d'une clé de pseudonymisation spécifique au projet par le responsable de pseudonymisation • Établissement d'un contrat de protection des données de type V • Inscription dans l'inventaire	• Attribution de l'autorisation d'utiliser la clé aux data consumers compétents • Pseudonymisation/appariement spécifique à chaque cas • Examen éventuel des données d'output par l'OFS	• Fin de validité de l'autorisation à utiliser la clé de pseudonymisation • Confirmation de la destruction des données	• Possibilité de simplifier la procédure pour les données non sensibles • Mesures de sécurité supplémentaires ou limitations dans la remise et/ou l'utilisation des données sensibles • Effacement des appariements de données sensibles une fois l'analyse terminée • Des tiers peuvent être associés à l'appariement, si nécessaire.

6.4 Sensibilité des données

Lors des appariements, il importe d'accorder une grande importance au degré de protection (à la sensibilité) des données, qu'il s'agisse des données qui sont appariées (données d'input) ou des données qui résultent de l'appariement (données d'output). Cette sensibilité détermine le caractère plus ou moins strict des mesures à prendre (restriction de la remise des données, suppression, etc.). Plus les données sont sensibles, plus leur protection doit être élevée. On distingue quatre niveaux de protection:

Degrés de protection

(tiré des «Directives relatives à la protection des données en cas de transmission de données individuelles à des tiers», état au 18.10.2006)

- **Degré 0 (données techniques) :**
Données ne se rapportant pas à une personne, par exemple des résultats de mesures.
- **Degré 1 (données personnelles simples) :**
Données dont la communication ne risque pas de porter atteinte à la personnalité des personnes physiques ou morales concernées (p. ex. le nom, le prénom, l'adresse, la date de naissance, la branche de l'entreprise). Combinées à des données sensibles, ces données peuvent toutefois requérir un degré de protection plus élevé (p. ex. les noms des personnes détenues dans un établissement pénitentiaire ou de la clientèle d'une clinique traitant des malades du sida). Souvent, les données du degré 1 sont assez facilement accessibles (via l'annuaire téléphonique, les rapports annuels et d'autres publications) et peuvent aussi être relevées par des tiers, indépendamment de l'OFS, moyennant une certaine charge.
- **Degré 2 (données personnelles qualifiées) :**
Données dont la communication présente un certain risque de porter atteinte à la personnalité des personnes physiques et morales concernées (p. ex. les données qui portent sur les revenus et la fortune, le loyer, les relations commerciales, la formation, l'activité professionnelle, les opinions et les comportements dans les domaines autres que ceux du degré 3).
- **Degré 3 (données personnelles sensibles) :**
Données dont la communication présente un risque majeur de porter atteinte à la personnalité des personnes physiques ou morales concernées (p. ex. indications sur la religion, sur les opinions et activités idéologiques, syndicales et politiques, la race, la santé, la sphère privée, l'aide sociale, les infractions).

La demande doit contenir des informations sur les critères mentionnés ci-dessous. Si un ou plusieurs critères ne sont pas remplis, une prise de position du délégué à la sécurité informatique est demandée dans cadre du processus afin de décider quelles mesures de sécurité supplémentaires doivent être prises le cas échéant.

Directives sur l'appariement

☐ ☐ Il ne s'agit pas d'un environnement de type cloud accessible au public⁹.

☐ ☐ Les données sont stockées en Suisse.

Les données sont cryptées :

☐ ☐ lors du transport

☐ ☐ lors du stockage

☐ ☐ L'accès physique à l'infrastructure est limité aux utilisateurs légitimes.

L'accès logique aux données est protégé par :

☐ ☐ une authentification à 2 facteurs et

☐ ☐ des droits d'accès limités aux utilisateurs légitimes.

☐ ☐ L'environnement est protégé par un pare-feu.

☐ ☐ Les autorisations d'accès sont contrôlées et tenues à jour.

☐ ☐ L'infrastructure est protégée contre les logiciels malveillants.

☐ ☐ Les vulnérabilités des logiciels sont surveillées et corrigées fréquemment (au moins 1x / an).

☐ ☐ Si des sauvegardes sont effectuées, elles doivent être cryptées.

⁹ Un environnement de type cloud accessible au public se réfère ici à un service cloud où tout utilisateur (personne ou entreprise) peut créer un compte comprenant un espace de stockage, (p.ex. Dropbox, Microsoft OneDrive, Google Drive, Apple iCloud, etc)

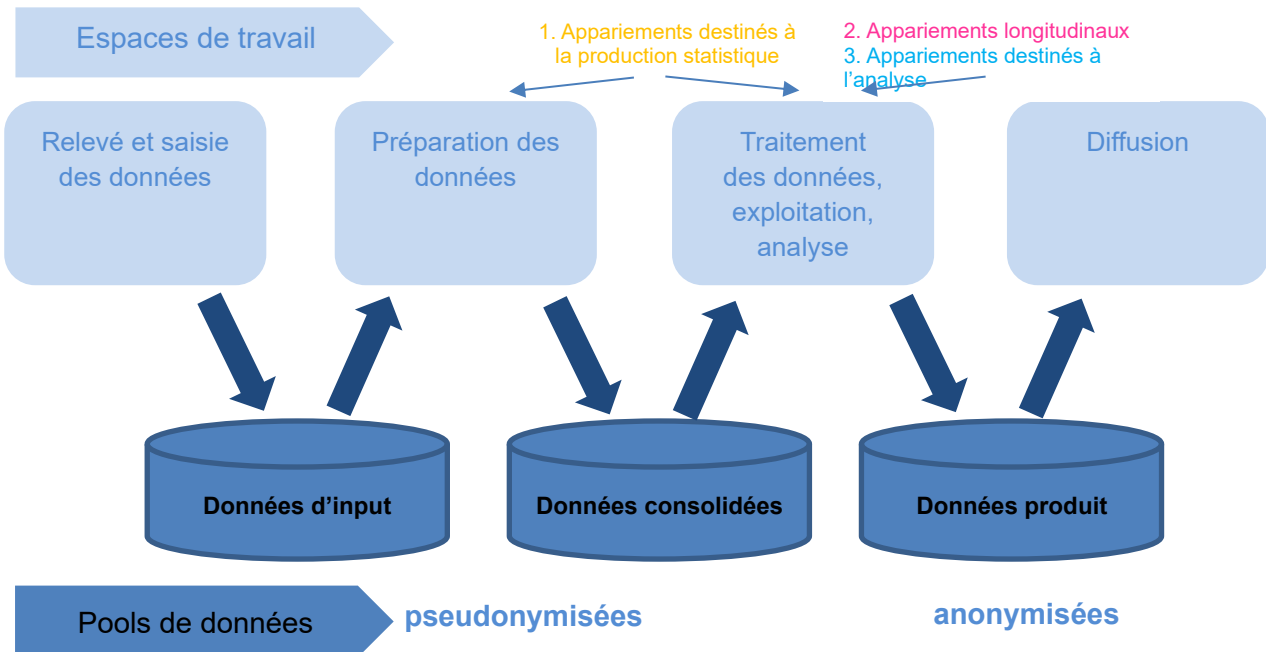
7 Production statistique, sécurité et appariement des données

7.1 Processus de production statistique

Dans la production statistique, on distingue généralement les étapes suivantes:

⇒ relevé et saisie des données ⇒ préparation des données ⇒ traitement des données, exploitation, analyse ⇒ diffusion.

Le schéma de base suivant s'applique à l'ensemble de la production statistique.



Voici comment se décomposent les étapes du processus

Relevé et saisie des données

- Réalisation de relevés (*registres, données administratives, etc.*) et des enquêtes, qui sont documentés par des projets, des descriptions d'interface des variables à collecter, etc. ou la reprise de données de sources administratives, de registres, de mesures, etc.
- Saisie des données.
- Enregistrement des données d'input (*les données d'input sont les données brutes* provenant des relevés. Elles contiennent normalement les caractères d'identification des personnes qui sont nécessaires à la préparation et aux éventuelles demandes de renseignements auprès des fournisseurs de données -> voir l'annexe 1. Ces données ne sont conservées que le temps nécessaire au processus de production statistique et sont préparées et pseudonymisées aussi vite que possible. Les données brutes originales sont ensuite détruites.

Préparation des données

- La préparation des données consiste à traiter les données d'input au niveau des incohérences et des valeurs manquantes ou extrêmes, et à calculer des variables synthétiques (caractères dérivés). Des appariements sont possibles à ce stade. Mais ils ne sont pas considérés comme tels, conformément à l'art. 28, al. 2, let. a OStatF. Il ne serait en effet ni efficace ni proportionné de respecter, lors de la préparation des données, les mesures strictes applicables aux appariements, en particulier la pseudonymisation préalable.
- Les données préparées sont stockées sous la forme de «données consolidées» (*les données consolidées sont des données individuelles qui ont été apurées. Elles sont conservées sous une forme pseudonymisée. Les variables d'identification (nom, adresse, etc.) sont supprimées et les identificateurs (numéro AVS, IDE, etc.) sont pseudonymisés (voir l'annexe 1). Les bonnes*

Directives sur l'appariement

pratiques demandent de stocker les données consolidées dans la banque de données centrale qui leur est destinée, conformément au concept SIS.

Traitement, exploitation et analyse des données

- Les données consolidées font l'objet d'autres opérations, telles que des opérations d'exploitation, d'analyse ou d'appariement (**appariements longitudinaux** ou **appariements destinés à l'analyse**).
- Ces diverses opérations se font en principe sur des données pseudonymisées.
- Les données qui en résultent ont valeur de «données de production» (*qui se présentent généralement sous une forme agrégée, et donc anonymisée -> voir l'annexe 1*) ou rejoignent les autres «données consolidées» si elles ne doivent pas être effacées en raison de leur caractère sensible (cf. art. 14a LSF).

Diffusion

- À partir des données de production, des articles de diffusion sont créés et mis à disposition sous une forme appropriée aux clients intéressés.
- Les données consolidées forment la base des produits de l'OFS (tableaux, cubes, datamarts pour des contrats de livraison des données ou des cartes, etc.).

Conservation des données

- Les données plausibilisées et pseudonymisées peuvent être conservées pendant 30 ans (100 ans dans des cas particuliers).

7.2 Protection des données

L'OFS garantit la protection et la sécurité des données conformément à la LSF, à la LPD, à l'OPDo et à la LSI en général et, dans le cas des appariements, conformément aux dispositions de l'OStatF, de l'ordonnance du DFI sur l'appariement de données et des présentes directives. Les appariements faisant l'objet d'un intérêt croissant de la part du public, cela oblige l'OFS à pratiquer la transparence sur ses activités, afin de préserver la confiance placée en lui.

Ses collaborateurs connaissent les avantages des appariements, mais aussi les risques qu'ils représentent, et sont en mesure d'informer le public de manière claire sur ses activités. Ils sont capables de répondre rapidement et de manière transparente et détaillée aux demandes d'information concernant les activités statistiques qui leur parviennent d'autres offices ou du PFPDT.

L'OFS est tenu d'appliquer la LSF, la LPD, le code de bonnes pratiques, la charte de la statistique publique et les directives concernant la sécurité informatique dans l'administration fédérale. Chaque collaborateur respecte les mesures prescrites par ces textes, par exemple en s'engageant par signature à respecter les [règles de comportement](#)¹⁰. Les unités organisationnelles déterminent un responsable de pseudonymisation pour leurs données. Cette personne assure la pseudonymisation des données consolidées et est responsable de l'accès aux clés de pseudonymisation de ces données ou aux clés spécifiques à des projets de recherche. Le chapitre 8 présente en détail la définition des rôles.

7.2.1 Espace de confiance de l'OFS

Le niveau de l'espace de confiance de l'OFS est défini par les lois pertinentes, la charte de la statistique publique et le code de bonnes pratiques. Ces textes, que tout le personnel de l'OFS est tenu d'appliquer, constituent le premier niveau de protection.

¹⁰ lien disponible uniquement à l'interne à l'OFS

Directives sur l'appariement

7.2.2 Secteurs – Droits d'accès aux données

Le niveau des secteurs correspond aux unités de production statistique à l'OFS. Leur but est la production, à partir des données collectées, de données consolidées destinées à être traitées, exploitées et analysées.

Les secteurs protègent les données en limitant et en contrôlant l'accès aux données d'input à traiter. Seuls les collaborateurs habilités ont accès aux données pour autant qu'elles soient pertinentes pour leur travail. La gestion des accès incombe aux sections de production.

7.2.3 Pseudonymisation des données consolidées – droits d'accès aux clés

La pseudonymisation des données consolidées empêche les appariements non autorisés de données individuelles consolidées (les pseudo-identificateurs sont propres à chaque processus de consolidation et ne sont pas compatibles avec les autres jeux de données consolidées). Le responsable de pseudonymisation règle l'attribution et la gestion des clés.

À chaque fois qu'une enquête périodique est effectuée, les données en résultant sont pseudonymisées à l'aide d'une nouvelle clé spécifique.

7.3 Pseudonymisation, dépseudonymisation et repseudonymisation

Les processus décrits ici se réfèrent au microservice de pseudonymisation de données (*Data Pseudonymisation Service*, DPS) et au logiciel de gestion de clés de chiffrement (*Keystore Management System*, KMS) développés dans le cadre du SIS. Les rôles correspondants sont décrits au chapitre 8.

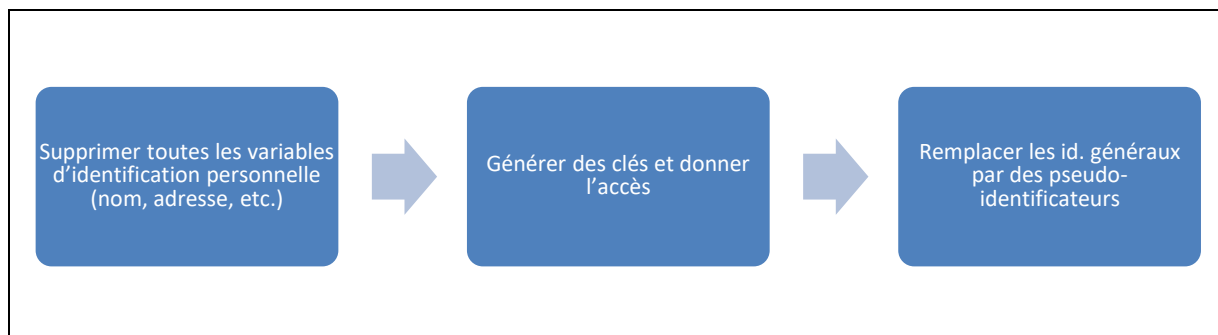
Pseudonymisation

La pseudonymisation consiste à supprimer tous les caractères personnels (p. ex. nom, adresse) d'un jeu de données qui permettent d'identifier la personne à laquelle il se rapporte et de remplacer les identificateurs originaires et transversaux (p. ex. numéro AVS) par un pseudo-identificateur attribué par l'OFS. Les données pseudonymisées ne permettent plus de remonter à la personne à laquelle elles se rattachent.

Les pseudo-identificateurs sont générés par un algorithme de cryptage. Les données qui se trouvent à l'extérieur du SIS doivent aussi être pseudonymisées au moyen de la solution proposée par le SIS. La pseudonymisation s'effectue au sein du SIS par la transformation de l'identificateur d'origine en un pseudo-identificateur, au moyen d'un processus à deux niveaux (niveau 1: clé OFS, niveau 2: clé sectorielle).

Des clés et des pseudo-identificateurs spécifiques sont en principe générés pour chaque production (relevé/enquête) de données consolidées. Cette méthode permet d'éviter que des jeux de données différents concernant une même personne puissent être appariés sans information supplémentaire. Les clés utilisées pour la pseudonymisation sont conservées dans un environnement spécialement sécurisé. Les clés sont générées et gérées par le responsable de pseudonymisation.

➔ **Processus de pseudonymisation**



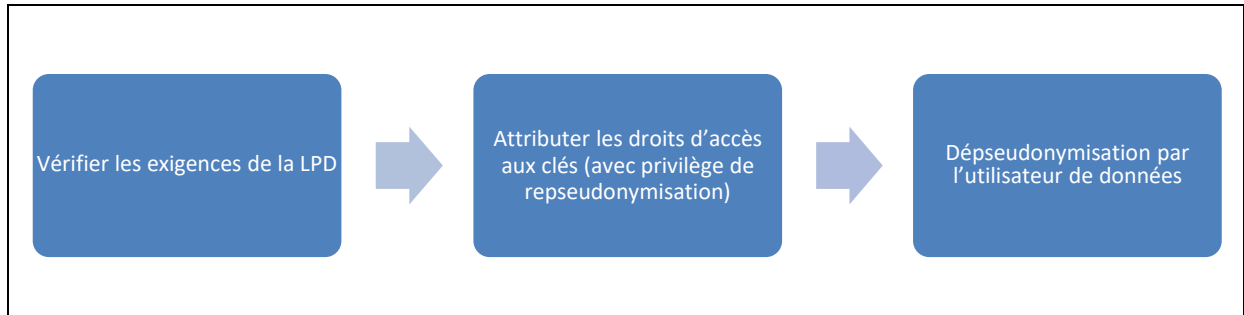
Directives sur l'appariement

Dépseudonymisation

Le processus inverse est la dépseudonymisation. La reconstitution des identificateurs d'origine (notamment les numéros AVS) est délicate du point de vue de la protection des données. Il convient donc d'examiner ceci au cas par cas, en particulier si la législation sur la protection des données peut être respectée (art. 25, al. 2 OStatF).

- Si le cas est fondé, le responsable de pseudonymisation autorise un utilisateur spécifique de données à accéder à la clé (avec privilège de dépseudonymisation).
- Les pseudo-identificateurs sont remplacés par les identificateurs originaux.

➔ Processus de dépseudonymisation

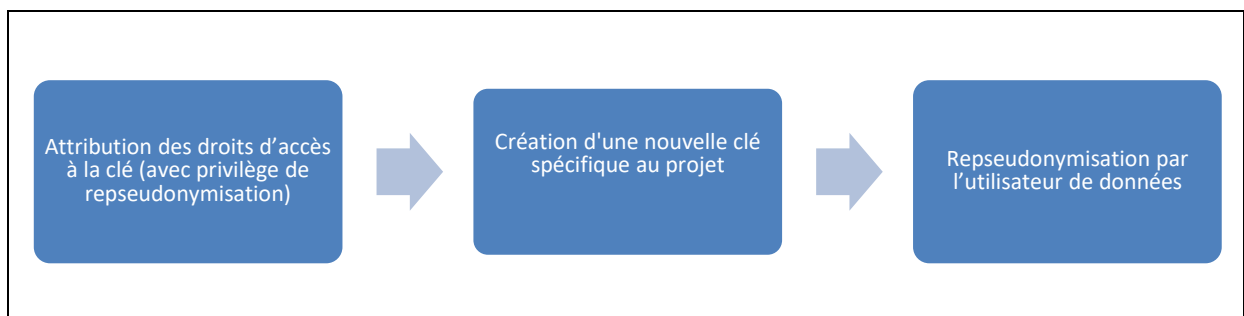


Repseudonymisation

Pour pouvoir appairer les données de différents relevés/secteurs, il faut d'abord les dépseudonymiser, à savoir décrypter les identificateurs, si les données ne proviennent pas du même secteur. Lorsque l'appariement concerne des données de l'OFS, la dépseudonymisation ne comporte qu'une étape (du niveau 2 au niveau 1). Les identificateurs d'origine sont reconstitués grâce aux identificateurs pseudonymisés, et ensuite remplacés par un identificateur spécifique au projet, ce qui permet d'appairer les différents jeux de données.

- Le responsable de pseudonymisation autorise un utilisateur spécifique de données à accéder à la clé (avec privilège de repseudonymisation).
- Le responsable de pseudonymisation crée une nouvelle clé spécifique au projet.
- Les pseudo-identificateurs sont remplacés par de nouveaux pseudo-identificateurs spécifiques au projet.

Processus de repseudonymisation



7.4 Principe de la gestion des clés de pseudonymisation

Seuls les détenteurs des clés de pseudonymisation, c'est-à-dire des droits d'accès correspondants, peuvent appairer des données. Le contrôle des appariements est garanti par la conservation des clés dans un environnement protégé et par leur gestion centralisée par les seules personnes autorisées.

Le concept

Les clés sont stockées de manière centralisée et sécurisée dans le système de gestion de clés de chiffrement (**Keystore Management System, KMS**). Le KMS est un microservice qui permet aux sections de production de créer et de gérer des clés et d'accorder des autorisations pour leur utilisation. L'accès aux clés gérées dans le KMS relève de la responsabilité du responsable de pseudonymisation.

L'administrateur KMS se charge de l'infrastructure centrale du KMS, la création des keystores ainsi que l'attribution du rôle de responsable de pseudonymisation.

Le responsable de pseudonymisation crée des clés et accorde les droits d'utilisation et d'accès (pseudonymisation, dépseudonymisation ou repseudonymisation) aux utilisateurs autorisés. L'OFS développe et exploite le KMS.

Une documentation au sujet du KMS est disponible uniquement en interne à l'OFS et se trouve sous <https://intranet.confluence.bfs.admin.ch/confluence/x/Awk2Eg>

8 Organisation et rôles

Tous les rôles décrits ici sont assumés par des membres du personnel de l'OFS.

Les désignations en anglais correspondent aux rôles définis dans le cadre du SIS. Elles se réfèrent au microservice de pseudonymisation des données DPS et au système de gestion de clés de chiffrement KMS.

Responsable du domaine thématique Production statistique

Le responsable du domaine thématique Production statistique est responsable des appariements au nom de l'OFS. Il peut consulter le conseil de direction avant de prendre une décision. Il décide de la réalisation des appariements destinés à la production de statistiques et à l'analyse, et fixe les éventuelles réserves et conditions.

Groupe de travail Appariements

Le groupe de travail Appariements est dirigé par un membre du conseil de direction. Il compte au moins un représentant de chaque division, du service juridique, de la section Méthodes statistiques, des services informatiques et du service d'appariement. Il se réunit en cas de nécessité, mais au moins deux fois par an.

Lors de sa séance du 9 décembre 2015, le conseil de direction a mandaté le groupe de travail pour les tâches suivantes:

Apporter un soutien, discuter et évaluer les travaux réalisés dans le cadre des appariements de données, en mettant l'accent sur les thèmes suivants:

- Orientation générale et conceptuelle des appariements de données et suivi des travaux
- Mise en œuvre opérationnelle et de l'organisation, y compris de l'informatique (technique, contenu et organisation)
- Bases légales, notamment sur la protection des données et les conditions méthodologiques
- Communication et transparence (interne et externe)

Directives sur l'appariement

Service d'appariement

Le service d'appariement est responsable des activités suivantes:

- Accompagner administrativement et coordonner les appariements de données. Cette activité inclut notamment le contrôle formel des demandes, l'élaboration et la transmission des avis internes (sous la forme d'une brève recommandation), la gestion des processus de décision, le pilotage, le contrôle formel et la documentation des projets d'appariement ainsi que les renseignements. Le service d'appariement n'a pas accès aux données à appairer.
- Débattre et émettre des recommandations, en cas de requête spéciale (au sujet du contenu, de la méthode, de la qualité, de la faisabilité et de l'éthique). Si nécessaire, faire appel à d'autres services (section Méthodes statistiques, service juridique, groupe de travail sur les appariements, etc.),
- gérer l'inventaire.

Responsable KMS

La ou le responsable KMS assume les tâches suivantes:

- Créer des keystores
- S'occuper de l'attribution et de la gestion du rôle de *responsable de pseudonymisation* et du *suppléant*.

Le rôle de responsable KMS peut être confié à plusieurs membres d'une même unité organisationnelle, à des fins de suppléance ou pour l'accomplissement de tâches communes par exemple. Il ne peut pas être cumulé avec les rôles de *responsable de pseudonymisation* et/ou *d'utilisateur de données*.

Responsable de pseudonymisation¹¹

Le responsable de pseudonymisation accomplit les tâches suivantes:

- Attribuer et gérer le rôle du *suppléant*
- Créer les clés de chiffrement au sein d'un keystore correspondant
- Gérer l'accès aux clés des personnes autorisées
- Il réalise la pseudonymisation et la dépseudonymisation, grâce aux droits que lui octroie le service d'appariement. Il est responsable de l'utilisation de la clé de chiffrement.
- Il assure la pseudonymisation des données consolidées. Il garantit que seules les personnes autorisées accèdent aux données consolidées.

Le rôle de responsable de pseudonymisation peut être confié à plusieurs membres d'une même unité organisationnelle, à des fins de suppléance par exemple (voir suppléant).

Responsable de pseudonymisation suppléant

Le suppléant a les mêmes tâches ou autorisations que le responsable de pseudonymisation, à ceci près qu'il ne peut pas gérer lui-même le rôle de suppléant.

Utilisateur de données (data consumer)

L'utilisateur de données exerce les tâches suivantes:

- Réaliser la pseudonymisation, la dépseudonymisation ou la repseudonymisation.

¹¹ Dans ce qui suit, les termes responsable de pseudonymisation ou utilisateur de données désignent les rôles et les droits d'accès qui y sont liés. Une même personne peut assumer différents rôles.

Directives sur l'appariement

Le rôle de l'utilisateur de données peut être confié à plusieurs membres d'une même unité organisationnelle, à des fins de suppléance ou pour l'accomplissement de tâches communes par exemple.

Autres rôles:

- Chef de division: cette personne est la première instance de décision pour toutes les demandes d'appariement internes et externes. Elle garantit l'expertise requise et la mise à disposition des ressources nécessaires à l'appariement.
- Sections métier: toutes les sections métier concernées de l'OFS examinent les demandes d'appariements internes et externes d'un point de vue technique.
- Service juridique: il examine la conformité juridique des demandes d'appariement internes et externes.
- Section Méthodes statistiques: elle examine si les demandes d'appariement internes et externes sont réalisables et correctes sur le plan de la méthode statistique.
- Section Informatique: elle est consultée en cas de besoin, par exemple en cas de désaccord sur la sécurité des données.

9 Éléments de l'appariement de données

9.1 Inventaires des appariements à l'OFS

Il existe trois catégories d'appariement à l'OFS (voir chap. 6.1.2). Le service d'appariement de l'OFS assure la gestion d'un inventaire¹² qui donne une vue d'ensemble de tous les appariements. La transparence et la protection des données sont ainsi garanties. Le chapitre 6.3 indique les conditions auxquelles chaque type d'appariement doit satisfaire.

Appariements destinés à la production statistique

Les appariements destinés à la production statistique sont traçables dans l'OStatF, car les sources de données sont indiquées pour chaque enquête et sondage. Dès que plusieurs sources de données sont concernées, il est évident qu'elles doivent être appariées. L'indication des appariements destinés à la production statistique a été ajoutée à l'ordonnance en 2014, à l'occasion de sa révision annuelle. Dans le cadre de la révision totale de l'ordonnance, on a renoncé à mentionner explicitement les appariements, car ils sont tous reconnaissables sur la base des sources mentionnées. De plus, chaque demande est répertoriée.

- Contexte: chaque appariement destiné à la production statistique doit faire l'objet d'une demande et est répertorié dans l'inventaire ad hoc.
- Méthode: révision annuelle de l'annexe de l'ordonnance. Les unités spécialisées sollicitent des appariements de manière continue. La marche à suivre est régie dans le présent document (voir chapitre 10 et annexe 5).
- Autorisation: décision du responsable du domaine thématique Production statistique et du Conseil fédéral concernant l'entrée en vigueur de l'ordonnance.

Appariements longitudinaux

Les appariements longitudinaux sont normalement moins sensibles que les appariements transversaux, du fait que les données proviennent du même relevé réalisé à des moments différents. De plus, contrairement au cas où plusieurs sources sont appariées, le risque d'identification des unités n'est pas considérablement accru. Le risque que des profils sensibles puissent en être dégagés n'en existe pas moins. Les appariements longitudinaux doivent être eux aussi dûment autorisés et soigneusement réalisés.

¹² L'inventaire n'est pas public, mais il est disponible sur demande.

Directives sur l'appariement

- Contexte: inventaire des appariements de données
- Responsable de la mise à jour permanente: service d'appariement
- Méthode: la marche à suivre est réglée dans le présent document (voir chapitre 10 et annexe 5).
- Autorisation: décision du service d'appariement

Appariements destinés à l'analyse de données

Normalement, les appariements destinés à l'analyse de données ne sont pas systématiques (c'est-à-dire qu'ils ne sont pas récurrents). Les demandes d'appariement de données peuvent émaner de l'OFS ou d'externes. L'ordonnance du DFI sur l'appariement de données (voir annexe 2, point 4) règle leur documentation par le service d'appariement.

- Contexte: inventaire des appariements de données
- Responsable de la mise à jour permanente: service d'appariement
- Méthode: la marche à suivre est réglée dans le présent document (voir chapitre 10 et annexe 5).
- Autorisation: décision du responsable du domaine thématique Production statistique

9.2 Demandes d'appariement

Toutes les demandes d'appariement doivent être déposées électroniquement (voir annexe 5), normalement auprès du service central d'appariement ou de la section concernée. Lorsqu'une telle demande est déposée auprès d'une section métier, il faut y associer immédiatement le service d'appariement.

Données requises

Le service d'appariement vérifie que la documentation accompagnant la demande est complète (informations sur le formulaire, informations du mandat de recherche, description des variables, etc.). Toute demande d'appariement, quelle que soit sa catégorie, doit contenir les informations suivantes:

- informations sur le demandeur (personne, institution),
- description du projet (y c. le but de l'appariement),
- données requises (données à appairer, caractéristiques; dans le cas de données externes, également les métadonnées et les bases légales),
- résultats visés (éventuellement publication prévue),
- délais, et
- données supplémentaires (type d'appariement - appariement unique ou récurrent, outils informatiques ou programmes spéciaux, etc.).

Processus

Les sections concernées, la section Méthodes statistiques et le service juridique de l'OFS examinent la demande d'appariement en vérifiant si elle est valable et réalisable des points de vue technique, méthodologique et juridique. Si nécessaire, le service d'appariement demande également à la section Informatique de l'OFS d'évaluer la demande.

Après avoir consulté le conseil de direction de l'OFS, le ou la responsable du domaine thématique Production statistique décide s'il est opportun de faire un appariement et si l'appariement sera fait.

Directives sur l'appariement

Documentation:

Toutes les demandes d'appariement et les appariements réalisés sont documentés. La documentation comprend les éléments suivants: •Demande •Évaluation •Décision •Contrat de protection des données. Elle se trouve dans GEVER.

Demandes d'appariement répétées

Lorsqu'un appariement a déjà fait l'objet d'une demande similaire, il est possible de renvoyer à la documentation fournie précédemment. Les éventuelles différences feront l'objet d'une description détaillée.

Durée de l'autorisation d'utiliser les clés de chiffrement

- Appariements internes à l'OFS: l'autorisation d'utiliser les identificateurs ou les clés nécessaires peut être accordée pour une durée déterminée pour ces cas. Les autorisations en question sont à renouveler périodiquement.
- Appariements pour des externes: la durée d'utilisation des données est définie contractuellement. Il est toutefois possible de demander une prolongation.

9.3 Règlement de traitement

Comme expliqué au chapitre 5, l'appariement en tant que tel ne requiert pas un règlement de traitement spécifique, qui viendrait compléter les présentes directives et les dispositions légales applicables. La nécessité de faire un tel règlement dépend plutôt du degré de protection des données d'entrée. Si les données d'entrée relèvent du niveau de protection 3, des règlements de traitement existent déjà.

9.4 Association de tiers aux travaux d'appariement

Conformément à l'art. 39, al. 4, OStatF, des tiers (personnes externes à l'OFS) peuvent être associés au processus d'appariement. L'OFS s'occupe toujours d'effectuer la pseudonymisation spécifique au projet ainsi que de créer et gérer la clé de chiffrement. Dans le cas où des tiers interviennent dans les étapes ultérieures du processus, l'OFS prend les mesures organisationnelles et techniques nécessaires pour garantir la protection et la sécurité des données (voir chapitre **Erreur ! Source du renvoi introuvable.**).

9.5 Appariements par les services de statistique régionaux

Conformément à l'art. 30, al. 2, let. a à e, OStatF, les services de statistique des cantons et des communes peuvent effectuer de manière autonome des appariements avec des données de la statistique fédérale, pour autant qu'ils remplissent les conditions requises. Ils doivent notamment garantir la protection et la sécurité des données au même degré que l'OFS, respecter les principes et les normes statistiques et être techniquement indépendants des organes exécutifs. Cette dernière condition est considérée comme remplie lorsqu'ils disposent d'une base légale régissant leur organisation et leur attribuant exclusivement une activité statistique, indépendante de toute activité de surveillance, d'exécution ou de réglementation, ou s'ils ont signé la Charte de la statistique publique de la Suisse de mars 2025 (cf. art. 4, al. 2, de l'ordonnance sur l'appariement de données).

Si ces services de statistique ont signé un contrat-cadre avec l'OFS, aucun contrat supplémentaire de protection des données n'est établi pour chaque appariement.

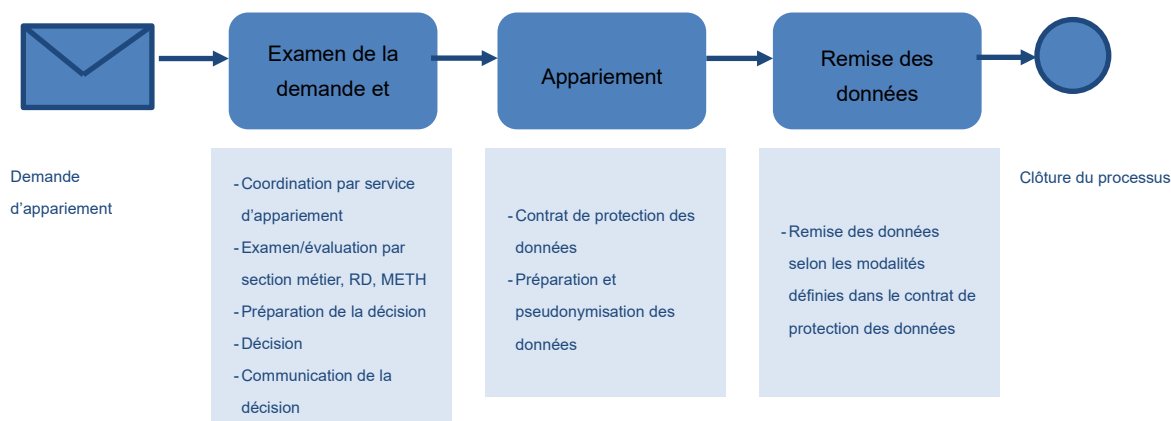
Mais, dans tous les cas, une demande doit être adressée à l'OFS. Si des appariements réguliers et récurrents sont nécessaires dans le cadre d'une production statistique, il est toutefois possible de déposer une demande qui régit les appariements récurrents sur le long terme.

10 Processus d'appariement

(voir également l'annexe 4 Description du processus)

10.1 Remarques préliminaires

L'appariement suit normalement les étapes suivantes:



Le processus comporte cinq étapes:

- Demande d'appariement,
- examen de la demande, avec décision indiquant si l'appariement peut être effectué, de quelle manière et quand (sauf dans le cas des appariements longitudinaux),
- réalisation de l'appariement,
- remise des données appariées,
- fin du processus d'appariement.

10.2 Vérification de la demande et prise de décision

10.2.1 Vérification de la demande

Les sections métier concernées (FACH), la section Méthodes statistiques (METH) et le service juridique (RD) évaluent la demande d'appariement. Dans le cas d'un appariement longitudinal, cette étape est supprimée.

Les rapports d'évaluation sont coordonnés par le service d'appariement. Ils comprennent deux volets:

- 1) une appréciation du projet fondée sur les spécificités du domaine.
- 2) une demande/recommandation à l'intention de l'instance décisionnelle.

La demande est d'abord transmise pour information aux responsables des divisions concernées. Les sections métier concernées, la section Méthodes statistiques et le service juridique de l'OFS examinent ensuite la demande d'appariement en vérifiant si elle est valable et réalisable du point de vue technique, méthodologique et juridique. Si nécessaire, le service d'appariement demande également à la section Informatique de l'OFS d'évaluer la demande. Après avoir consulté le conseil de direction de l'OFS, le ou la responsable du domaine thématique Production statistique décide de la recevabilité de la demande et de l'acceptation de l'appariement.

L'examen de la demande tient compte du risque d'identification des individus, c'est-à-dire de dépseudonymisation. Il convient de noter qu'il est pratiquement impossible d'anonymiser complètement les données individuelles. La pseudonymisation spécifique au projet, la limitation aux

Directives sur l'appariement

variables strictement nécessaires et l'agrégation maximale du niveau de détail des variables potentiellement identifiantes constituent un obstacle technique dans ce domaine.

Évaluations

Prise de position du SERVICE D'APPARIEMENT: la demande est-elle complète? Remarques?

Évaluation SECTION(S) MÉTIER: les données et les identificateurs sont-ils disponibles?

L'appariement est-il pertinent, fait-t-il sens ...? L'appariement est-il faisable (du point de vue méthodologique, technique)? S'agit-il de données sensibles (input/output)? Quel est le coût de l'appariement/quelles sont les ressources disponibles? Procédure (qui fait quoi, quand et comment)? Conditions, réserves/restrictions (dispositions spéciales, utilisation des données de l'output, ...)?

Évaluation par METH: Le projet est-il correct/défendable du point de vue méthodologique? Évaluation de la sensibilité des données et du degré de protection (données de l'input + résultats)? Les résultats font-ils sens? Y a-t-il des réserves/restrictions?

Évaluation par RD: Les conditions juridiques sont-elles réunies? Réserves, exigences/dispositions spéciales?

Dans de rares cas (p. ex. stockage des données sur un cloud), une *évaluation par la section IT* est également nécessaire.

(⇒ voir annexe 5 Formulaire)

10.2.2 Décision

Sur la base de la demande soumise au conseil de direction de l'OFS ou de la recommandation des instances d'évaluation, la personne responsable du domaine thématique Production statistique décide si l'appariement peut avoir lieu, quelle forme il doit prendre, si des allègements sont possibles ou s'il faut au contraire émettre des réserves (p. ex. mesures spéciales, exigences supplémentaires, réserves quant à l'utilisation des données appariées, à la conservation ou suppression des données, aux délais).

- Les décisions sont prises par écrit.
- Le demandeur est informé par écrit de la décision et de l'évaluation par la section responsable. Tout refus est motivé.
Si le demandeur estime injustifiés les motifs du refus, il peut demander que la décision soit reconsidérée.
- Une décision positive du responsable du domaine Production statistique autorise le responsable de pseudonymisation à générer et à remettre les clés de chiffrement, à la condition que les réserves émises soient respectées.

Le processus est simplifié dans le cas d'appariements longitudinaux. La décision est prise par le service d'appariement.

(⇒ voir annexe 5 Formulaire)

Directives sur l'appariement

Possibles réserves et allègements en ce qui concerne la décision du responsable du domaine thématique Production statistique:

Réserves:

Dans le cas de données sensibles, la décision peut imposer

- des mesures (de sécurité) spéciales lors de la réalisation des appariements,
- des restrictions à la communication ou à l'utilisation des données.

Allègements:

- Lorsqu'un appariement est destiné à la production d'une statistique récurrente, une autorisation peut être délivrée pour une certaine durée. Sa durée est déterminée d'après la nature de la production statistique et la sensibilité des données. La décision à cet égard est laissée à la discrétion du responsable du domaine thématique Production statistique.
- Des allègements peuvent être décidés en fonction de la sensibilité des données, du genre de mandant ou de demande d'appariement. Ils sont laissés à la discrétion du responsable du domaine thématique Production statistique.

10.3 Réalisation de l'appariement

L'appariement est dirigé par la section responsable des données. Lorsque les données concernent différentes sections, ces dernières se répartissent le *lead*, les rôles et les responsabilités. Si aucune donnée de l'OFS n'est concernée, le lead est assumé par une section qui connaît les données concernées ou qui est familiarisée avec le thème des analyses.

10.3.1 Étapes de l'appariement

Les appariements sont normalement effectués par l'OFS. L'OFS s'occupe toujours d'effectuer la pseudonymisation spécifique au projet ainsi que de créer et gérer la clé de chiffrement. Idéalement, l'appariement se fait selon les étapes suivantes:

- ***Mettre les données à disposition:***

Les données de l'OFS sont préparées par les utilisateurs de données concernés. L'OFS réceptionne les données externes (données tierces et autres données). Ces données (données de l'OFS ainsi que les autres données ou données de tiers) contiennent un identificateur approprié pour l'appariement (p. ex. numéro AVS) ou peuvent être dépseudonymisées afin de retourner à cet identificateur original ~~en fonction de cet~~ identificateur.

- ***Créer une clé spécifique au projet:***

Le responsable de pseudonymisation de l'unité en charge du projet génère une clé spécifique au projet et attribue le droit d'utilisation (avec privilège de repseudonymisation) aux utilisateurs de données concernés.

- ***Pseudonymiser les données:***

Les données sont pseudonymisées via l'infrastructure interne de l'OFS. Les identificateurs communs spécifiques au projet permettent de relier les différentes données individuelles entre elles. Le transfert aux utilisateurs de données se fait par un canal sécurisé.

- ***Relier les données entre elles:***

Les différents jeux de données sont reliés entre eux grâce au pseudo-identificateur spécifique au projet. Cette étape est généralement effectuée par le demandeur.

Un document relatif à la structure de l'infrastructure de pseudonymisation est disponible (interne à

l'OFS) sous <https://intranet.confluence.bfs.admin.ch/confluence/x/NQc2Eq>¹³.

10.3.2 Appariement par des services cantonaux ou communaux

Les services de statistique cantonaux ou communaux peuvent être autorisés, à certaines conditions, à réaliser eux-mêmes des appariements à partir de données de la statistique fédérale – même sous une forme non pseudonymisée – (voir art. 14a, al. 2 LSF, art. 30, al. 2, OStatF et art. 4 de l'ordonnance du DFI sur l'appariement de données). Si ces conditions sont remplies, qu'un règlement de traitement adéquat a été établi et qu'un contrat de protection des données et d'appariement a été signé par les deux parties, il reste à la section métier responsable à livrer les données éventuellement requises (avec un identificateur approprié) et à vérifier que les accords contractuels relatifs à la protection et à l'utilisation des données sont respectés.

10.4 Remise de données appariées

La communication de données appariées est soumise aux mêmes règles que la remise des autres données individuelles. On observera à cet égard, outre les dispositions des lois et des ordonnances, en particulier les «*Directives relatives à la protection des données en cas de transmission de données individuelles à des tiers*» (état au 18.10.2006).

Les détails de la remise de données individuelles sont à régler dans tous les cas par contrat.

10.5 Clôture du projet d'appariement et effacement des données appariées

Une fois que les données appariées sont disponibles et qu'elles ont été utilisées conformément à l'accord, le processus d'appariement est terminé. Il reste à observer les obligations suivantes:

- l'autorisation d'utiliser les clés d'appariement spécifiques au projet prend fin.

En raison de la protection des données, les données appariées doivent également être *détruites* après la fin de leur exploitation statistique si elles contiennent des *données sensibles* ou des *profils de la personnalité* (voir art. 14a LSF et art. 33 OStatF). La décision de détruire ou d'effacer les données est réglée dans la décision d'appariement (voir chapitre 10.2.2), à la rubrique «Spécifications, réserves».

¹³ lien disponible uniquement à l'interne à l'OFS

Facteurs spéciaux

Différents facteurs doivent être pris en compte au moment d'évaluer la pertinence d'un appariement car ils peuvent en influencer concrètement le processus. Il s'agit notamment des facteurs suivants:

► **Demandeur:** on distingue les catégories suivantes:

- les demandeurs internes (unités organisationnelles de l'OFS),
- les demandeurs externes (p. ex. autres services fédéraux, cantonaux et communaux, instituts de recherche, tiers),
- les offices statistiques des cantons et des communes qui font partie des services habilités à effectuer des appariements.

► **Données à appairer** (p. ex. nature, origine, sensibilité des données). En ce qui concerne l'origine des données, on opère les distinctions suivantes (voir annexe 1 Définitions, Concept du SIS):

- A)** Données de l'OFS (données dont l'OFS est propriétaire) ⇒ **données de l'OFS**.
- B)** Données relevées dans le cadre de la LSF et de l'ordonnance sur la statistique fédérale qui ne sont pas la propriété de l'OFS (p. ex. données d'autres offices fédéraux) ⇒ **données tierces**.
- C)** Données qui ne sont pas relevées en vertu de la LSF (p. ex. données administratives de services de l'administration ou d'autorités; données relevées par des chercheurs ou d'autres tiers) ⇒ **autres données**

Ces différentes combinaisons débouchent sur autant de variantes qu'il n'est pas utile de décrire en détail et de catégoriser.

11 Annexes

11.1 Annexe 1: Définitions (concept SIS)

Définitions selon le glossaire OFS - NaDB¹⁴

Les domaines suivants s'inscrivent dans la chaîne de valorisation et correspondent aux concepts du SIS:

Données d'input

Par données d'input (aussi appelées données brutes), on entend les données qui proviennent des fournisseurs de données et de l'exécution des relevés de l'OFS et qui ont été acceptées par l'OFS. Leur principale caractéristique est qu'elles n'ont pas encore été traitées et qu'elles se présentent donc sous une forme brute.

Un autre critère déterminant ici est celui du responsable des données. Il faut distinguer entre deux types de données d'input:

a) *Données résultant de relevés exécutés ou mandatés par l'OFS:*

Il s'agit de données relevées par l'OFS lui-même ou par des institutions externes mandatées par l'OFS. L'OFS dispose de ces données sous une forme brute et doit encore les contrôler et les valider.

Ces données peuvent être des données primaires (données issues des relevés réalisés ou mandatés par l'OFS à des fins statistiques) ou des données secondaires (en particulier, des données des registres tenus par l'OFS).

b) *Données de relevés externes et données externes:*

Ces données ne proviennent pas de relevés effectués par l'OFS ou sur mandat de ce dernier, mais par d'autres offices, institutions publiques ou autres, qui livrent des données déjà traitées (généralement validées, plus rarement agrégées ou traitées dans un autre contexte).

Ces données n'ayant pas été collectées à des fins statistiques, elles sont souvent incomplètes. Il incombe à l'OFS d'en combler les lacunes. En revanche, les données externes déjà traitées (en particulier celles qui sont agrégées) ne peuvent généralement plus être validées.

Parmi ces autres données, on trouve aussi bien les données primaires qui n'ont pas été saisies par l'OFS ou ses mandataires et toutes les données secondaires (qui ne visent pas des fins statistiques). Les données d'input comprennent plus largement les données concernant les produits et les objets d'information des fournisseurs de données externes.

Étant donné que ces données (modifiées pour servir des fins statistiques) n'appartiennent plus à leur fournisseur primaire, l'OFS en devient leur propriétaire dans les limites d'une utilisation statistique.

Données consolidées

Les données consolidées sont des données individuelles ou microdonnées.

Il s'agit de données pseudonymisées qui ont été traitées selon le processus de préparation statistique des données (PPSD) et qui sont disponibles pour l'analyse. Les données consolidées peuvent contenir des caractères dérivés, telles que l'âge, la catégorie socioprofessionnelle, le haut niveau de formation achevé.

Les *données agrégées* en sont toutefois *exclues*.

Données produit

Les données de production sont normalement le résultat d'une analyse ou d'une interprétation. Elles servent de base aux étapes suivantes de publication. Elles comprennent aussi les données préparées

¹⁴ <https://intranet.confluence.bfs.admin.ch/confluence/x/SwWECg>

Directives sur l'appariement

spécialement à l'intention d'un ou de plusieurs demandeurs (à des fins d'anonymisation, p. ex.). Les métadonnées relatives à la qualité des données (estimation de la variance, proportion d'utilisations, proportion de valeurs manquantes, etc.) doivent également être incluses dans les données de production.

Données destinées à la publication

Sont considérées comme données destinées à la publication:

- toutes les données standard dont l'utilisation publique est autorisée,
- les données fournies directement à des tiers (articles individualisés) et
- ce que l'on appelle les objets d'information.

1. Les données destinées à la publication ne sont pas seulement des «produits de visualisation», mais aussi des données consolidées (traitées ou éditées), des données produit ou des métadonnées (registres, nomenclatures, etc.).

11.2 Annexe 2: Bases légales

1. Loi sur la statistique fédérale (LSF; RS 431.01).

Art. 14a *Appariement de données*

1 Pour exécuter ses tâches en matière de statistiques, l'office peut appairer des données à condition de les rendre anonymes. Si des données sensibles sont appariées ou si l'appariement des données permet d'établir des profils de la personnalité, les données appariées doivent être effacées une fois les travaux statistiques d'exploitation terminés. Le Conseil fédéral règle les modalités.

2 Les services cantonaux et communaux de statistique ne sont autorisés à appairer les données de l'office avec d'autres données pour exécuter leurs tâches en matière de statistiques qu'avec l'accord écrit de ce dernier et aux conditions qu'il aura fixées.

2. Loi sur l'harmonisation de registres (LHR; RS 431.02)

Art. 16 *Utilisation des données par l'office à des fins statistiques, de recherche et de planification*

1 L'office peut utiliser les données pour effectuer des relevés ou des exploitations statistiques.

2 Il peut tirer des échantillons à partir des données pour effectuer des relevés statistiques.

3 Il peut utiliser les données mentionnées à l'art. 6, let. a à h, j, k et m, pour constituer un répertoire d'adresses pour l'exécution de relevés statistiques.

4 Il peut, pour remplir ses tâches en matière de statistiques, appairer les données dépourvues de désignation de personne avec celles du RegBL et du Registre des entreprises et des établissements (REE) et les conserver durablement.

3. Loi fédérale sur la protection des données (LPD; RS 235.1).

Art. 39 *Traitements à des fins ne se rapportant pas à des personnes*

1 Les organes fédéraux sont en droit de traiter des données personnelles à des fins ne se rapportant pas à des personnes, notamment dans le cadre de la recherche, de la planification ou de la statistique, si les conditions suivantes sont réunies:

- a. les données sont rendues anonymes dès que la finalité du traitement le permet;
- b. l'organe fédéral ne communique des données sensibles à des personnes privées que sous une forme ne permettant pas d'identifier les personnes concernées;
- c. le destinataire ne communique les données à des tiers qu'avec le consentement de l'organe fédéral qui les lui a transmises; et
- d. les résultats du traitement sont publiés sous une forme ne permettant pas d'identifier les personnes concernées.

2 Les art. 6, al. 3, 34, al. 2, et 36, al. 1, ne sont pas applicables.

4. Ordonnance sur la statistique fédérale (OStatF; RS 431.011)

Section 6: Appariement de données

Art. 28 *Définition*

1 On entend par appariement de données le fait de relier des données provenant de sources différentes, telles que données d'enquêtes, données de registres, données administratives ou données de mesures.

2 Ne sont pas considérés comme un appariement au sens de l'al. 1:

- a. le recoupement de données avec d'autres sources dans le cadre de leur préparation conformément à l'art. 25, y compris à des fins de test;
- b. le fait de relier des données agrégées de différentes sources, notamment pour l'établissement de statistiques de synthèse.

Art. 29 *Principes généraux*

1 Les appariements servent à obtenir des nouvelles informations statistiques sans avoir à effectuer de relevés et d'enquêtes.

2 Pour exécuter ses tâches statistiques, l'OFS peut appairer aussi bien ses propres données que celles sur lesquelles il n'a aucun droit (données tierces).

3 En cas de demande régulière de la part des chercheurs et d'autres offices, il peut réaliser des appariements sous forme de produits standards.

Art. 30 *Conditions*

Directives sur l'appariement

1 Des appariements ne peuvent être effectués que si les conditions suivantes sont réunies:

- a. ils sont appropriés et nécessaires à l'accomplissement de travaux statistiques; et
- b. les données concernées présentent les caractéristiques et la qualité requises pour un traitement statistique.

2 Les services statistiques des cantons et des communes sont autorisés, pour exécuter leurs tâches statistiques, à appairer des données de l'OFS entre elles ou avec leurs propres données, pour autant qu'ils s'engagent, dans un contrat de protection des données:

- a. à garantir la protection des données au même degré que l'OFS;
- b. à prendre des mesures suffisantes pour garantir la sécurité des données;
- c. à respecter les principes et les normes statistiques;
- d. à édicter et mettre en œuvre, avant la communication des données, un règlement de traitement des données, et
- e. à garantir leur indépendance professionnelle vis-à-vis des organes exécutifs.

3. Le DFI définit à quelles conditions les principes et les normes statistiques sont réputés respectés et à quelles conditions l'indépendance professionnelle des services statistiques des cantons et communes par rapport aux organes exécutifs est garantie.

Art. 31 Communication de données appariées

Lorsque la loi prévoit que les données peuvent être communiquées à des fins ne se rapportant pas à des personnes, notamment à des fins de recherche, de planification et de statistique, l'OFS peut communiquer des données appariées conformément à l'art. 37.

Art. 32 Anonymisation et destruction des données appariées

(Art. 14a LSF)

1. Des données appariées peuvent être conservées sous forme pseudonymisée après la fin de leur exploitation statistique initiale si elles sont continuellement analysées dans le cadre de séries de longue durée.
2. Elles doivent être anonymisées dès que les données sources de la dernière collecte ont été intégrées à l'analyse. S'il s'agit de données sensibles ou si l'appariement de données permet d'établir les caractéristiques essentielles d'une personne physique ou morale, elles doivent être détruites.

Art. 33 Reproductibilité de projets de recherche

1. Lorsque des projets de recherche d'importance nationale utilisent des données sensibles ou permettent d'établir les caractéristiques essentielles d'une personne physique ou morale, l'OFS peut, sur demande des unités et tiers visés à l'art. 39, sauvegarder les données des différentes sources et la clé utilisée pour créer l'identificateur propre au projet, afin de garantir la reproductibilité du projet tout en détruisant les données appariées. Les données et la clé doivent être conservées séparément.
2. Toute personne souhaitant reproduire un appariement de données doit en faire la demande auprès de l'OFS.

Art. 34 Sécurité des données

Le DFI définit les exigences en matière de sécurité des données.

4. Ordonnance du DFI concernant l'appariement de données statistiques (Ordonnance sur l'appariement de données; RS 431.012.13).

Art. 1 Exigences en matière de sécurité des données

¹ Pour chaque projet d'appariement de données provenant de différentes sources, l'Office fédéral de la statistique (OFS) établit un pseudo-identificateur et génère les clés nécessaires.

² Les clés sont conservées de manière centralisée et sécurisée.

³ Tout octroi de clé est journalisé.

Art. 2 Demande d'appariement de données

¹ La demande d'appariement de données (art. 39, al. 1, OStatF) doit être motivée; elle doit être soumise par voie électronique.

² En vue d'un appariement devant inclure des jeux de données non gérés par l'OFS, le demandeur doit joindre à sa demande les indications prévues à l'art. 39, al. 3, OStatF et l'accord du service responsable des jeux de données en question.

³ L'OFS examine la demande et prend une décision.

Directives sur l'appariement

Art. 3 Participation des demandeurs au processus

¹ Le demandeur transmet à l'OFS les données nécessaires à l'appariement.

² L'OFS remet au demandeur les données munies d'un pseudo-identificateur spécifique au projet. Le demandeur met en relation les données (matching).

³ L'OFS définit dans quels cas les tâches visées à l'art. 39, al. 4, OStatF doivent être effectuées à un poste de travail sécurisé dans ses locaux.

Art. 4 Services statistiques des cantons et des communes

¹ Les principes et normes statistiques visés à l'art. 30, al. 2, let. c, OStatF sont réputés respectés lorsque les services statistiques des cantons et des communes accomplissent tous les travaux statistiques dans le respect de l'indépendance professionnelle, de l'objectivité, de l'impartialité, de la fiabilité, de la confidentialité et de l'efficacité au regard des coûts.

² L'indépendance professionnelle des services de statistique par rapport aux organes exécutifs au sens de l'art. 30, al. 2, let. e, OStatF est considérée comme acquise lorsque les services de statistique sont partenaires du système statistique fédéral ou remplissent l'une des conditions suivantes:

- a. ils disposent d'une base légale régissant leur organisation et leur attribuant exclusivement une activité statistique, indépendante de toute activité de surveillance, d'exécution ou de réglementation,
- b. ils ont signé la Charte de la statistique publique de la Suisse de mars 2025¹⁵.

5 Ordonnance sur la protection des données (OPDo; RS 235.11)

Art. 3 Mesures techniques et organisationnelles

1 Pour assurer la confidentialité, le responsable du traitement et le sous-traitant prennent des mesures appropriées afin que:

- a. les personnes autorisées n'aient accès qu'aux données personnelles dont elles ont besoin pour accomplir leurs tâches (contrôle de l'accès aux données);
- b. seules les personnes autorisées puissent accéder aux locaux et aux installations utilisés pour le traitement de données (contrôle de l'accès aux locaux et aux installations);
- c. les personnes non autorisées ne puissent pas utiliser les systèmes de traitement automatisé de données personnelles à l'aide d'installations de transmission (contrôle d'utilisation).

2 Pour assurer la disponibilité et l'intégrité, le responsable du traitement et le sous-traitant prennent des mesures appropriées afin que:

- a. les personnes non autorisées ne puissent pas lire, copier, modifier, déplacer, effacer ou détruire des supports de données (contrôle des supports de données);
- b. les personnes non autorisées ne puissent pas enregistrer, lire, modifier, effacer ou détruire des données personnelles dans la mémoire (contrôle de la mémoire);
- c. les personnes non autorisées ne puissent pas lire, copier, modifier, effacer ou détruire des données personnelles lors de leur communication ou lors du transport de supports de données (contrôle du transport);
- d. la disponibilité des données personnelles et l'accès à celles-ci puissent être rapidement restaurés en cas d'incident physique ou technique (restauration);
- e. toutes les fonctions du système de traitement automatisé de données personnelles soient disponibles (disponibilité), que les dysfonctionnements soient signalés (fiabilité) et que les données personnelles stockées ne puissent pas être endommagées en cas de dysfonctionnements du système (intégrité des données);
- f. les systèmes d'exploitation et les logiciels d'application soient toujours maintenus à jour en matière de sécurité et que les failles critiques connues soient corrigées (sécurité du système).

3 Pour assurer la traçabilité, le responsable du traitement et le sous-traitant prennent des mesures appropriées afin que:

- a. il soit possible de vérifier quelles données personnelles sont saisies ou modifiées dans le système de traitement automatisé de données, par quelle personne et à quel moment (contrôle de la saisie);
- b. il soit possible de vérifier à qui sont communiquées les données personnelles à l'aide d'installations de transmission (contrôle de la communication);
- c. les violations de la sécurité des données puissent être rapidement détectées (détection) et que des mesures puissent être prises pour atténuer ou éliminer les conséquences (réparation).

¹⁵ La charte peut être consultée gratuitement sur le site de l'Office fédéral de la statistique à l'adresse suivante: www.bfs.admin.ch > À propos de nous > Engagement qualité > Contexte national.

Directives sur l'appariement

Art. 4 Journalisation

1 Lors de traitements automatisés de données sensibles à grande échelle ou de profilages à risque élevé et lorsque les mesures préventives ne suffisent pas à garantir la protection des données, le responsable du traitement privé et son sous-traitant privé journalisent au moins l'enregistrement, la modification, la communication, l'effacement et la destruction des données ainsi que l'accès aux données. La journalisation est notamment nécessaire lorsque, sans cette mesure, il n'est pas possible de vérifier a posteriori que les données ont été traitées conformément aux finalités pour lesquelles elles ont été collectées ou communiquées.

2 Lors du traitement automatisé de données sensibles, de profilages et de traitements automatisés de données soumis à la directive (UE) 2016/680, l'organe fédéral responsable et son sous-traitant journalisent au moins l'enregistrement, la modification, la communication, l'effacement et la destruction des données ainsi que l'accès aux données. Lors d'autres traitements automatisés de données, ils évaluent au préalable le risque pour les droits fondamentaux des personnes concernées. Ils déterminent sur cette base, ainsi qu'en tenant compte de l'état des connaissances et des coûts de mise en œuvre, si et dans quelle mesure les opérations précitées doivent être journalisées. Pour l'évaluation du risque, ils tiennent notamment compte du type de données traitées, ainsi que de la finalité, de la nature, de l'étendue et des circonstances du traitement.

2^{bis} L'examen de la journalisation au sens de l'al. 2 est consigné par écrit. Le résultat et le contenu de l'examen sont communiqués, sur demande, au Préposé fédéral à la protection des données et à la transparence (PFPDT).

3 Pour les données personnelles accessibles à tout un chacun, l'enregistrement, la modification, l'effacement et la destruction des données doivent au moins être journalisés dans les cas prévus aux al. 1 et 2, 1^{re} phrase.

4 La journalisation doit fournir des informations sur l'identité de la personne qui a effectué le traitement, la nature, la date et l'heure du traitement et, cas échéant, l'identité du destinataire des données.

5 Les procès-verbaux de journalisation sont conservés durant au moins un an, séparément du système dans lequel les données personnelles sont traitées. Ils sont accessibles uniquement aux organes et aux personnes chargés de vérifier l'application des dispositions relatives à la protection des données personnelles ou de préserver ou restaurer la confidentialité, l'intégrité, la disponibilité et la traçabilité des données, et ne peuvent être utilisés qu'à cette fin.

5. Section: Traitements des données à des fins ne se rapportant pas à des personnes

Art. 35

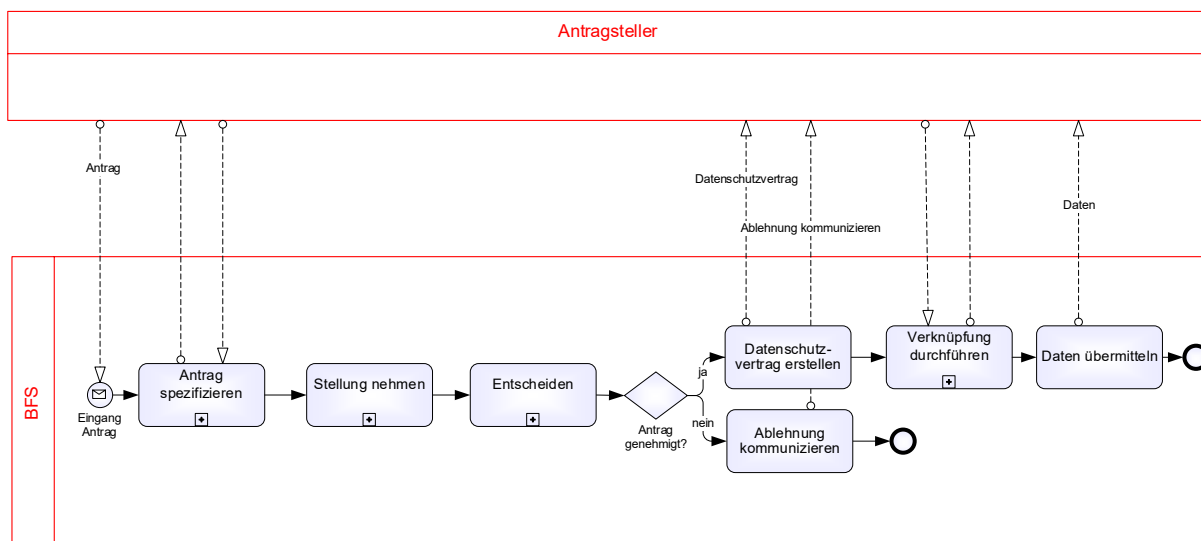
Lorsque des données personnelles sont traitées à des fins ne se rapportant pas à des personnes, en particulier à des fins de recherche, de planification ou de statistique, et que le traitement sert également une autre finalité, les dérogations prévues à l'art. 39, al. 2, LPD ne s'appliquent qu'au seul traitement effectué à des fins ne se rapportant pas à des personnes.

Art. 42 Registre des activités de traitement des organes fédéraux

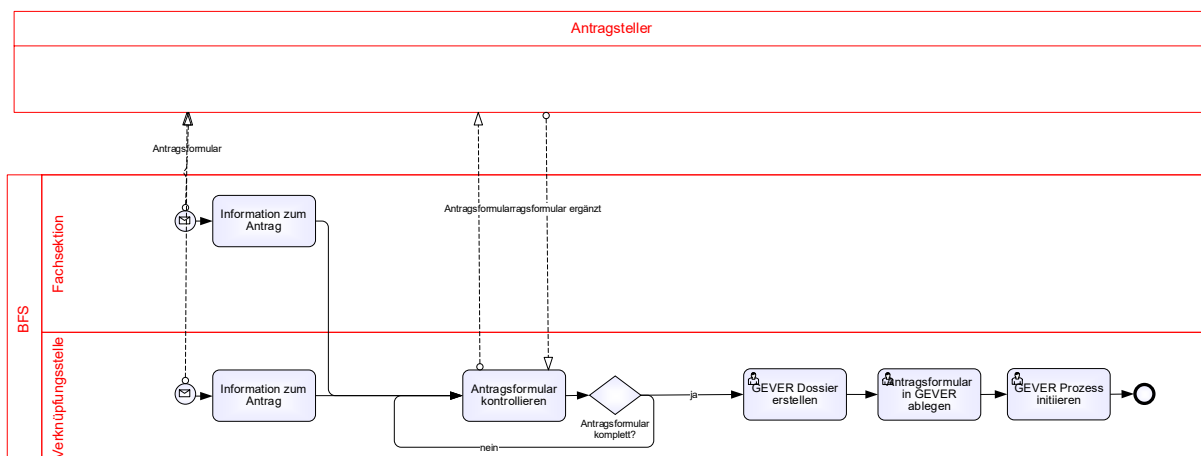
1. Le registre des activités de traitement des organes fédéraux contient les informations fournies par les organes fédéraux conformément aux art. 12, al. 2, LPD et 31, al. 2, de la présente ordonnance. 2. Il est publié en ligne. Les inscriptions au registre concernant les activités de traitement automatisé prévues, au sens de l'art. 31, ne sont pas publiées.

11.3 Annexe 3: Description des processus (voir aussi chapitre 10)

11.3.1 Traitement de la demande (vue globale)

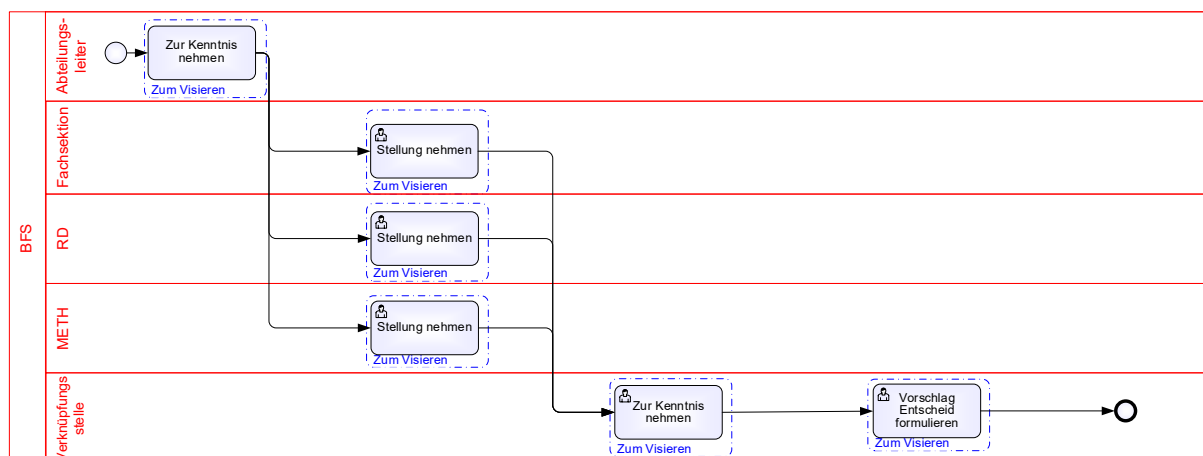


11.3.2 Précision de la demande

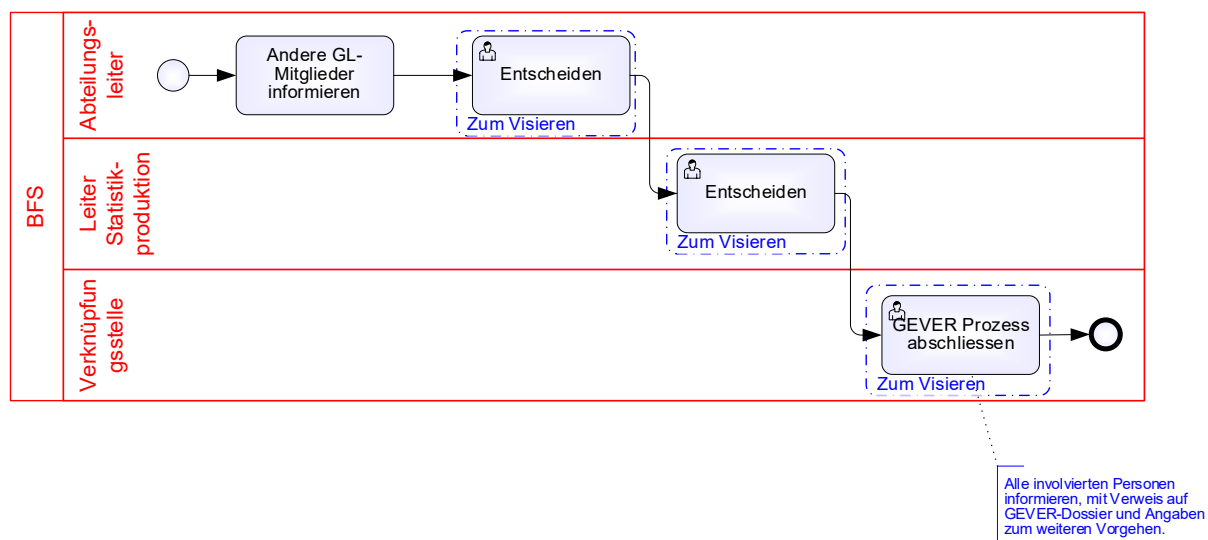


Directives sur l'appariement

11.3.3 Prise de position

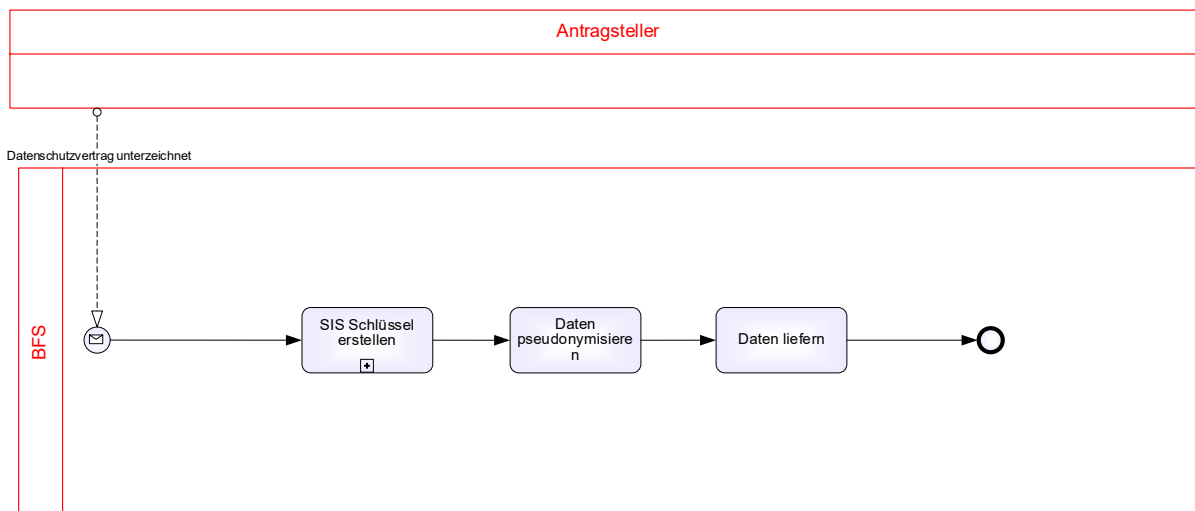


11.3.4 Décision

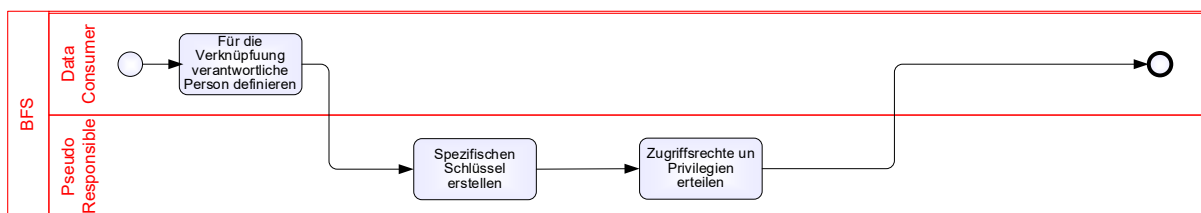


Directives sur l'appariement

11.3.5 Réalisation de l'appariement



11.3.6 Création clé SIS



Remarque: Cette documentation de processus a été réalisée avec Microsoft Visio. Le fichier original (interne à l'OFS) se trouve sous [Processus \(214.0-00667/00001\)](#)

Directives sur l'appariement

11.4 Annexe 4: Formulaire

Demande, évaluation et décision:

<https://www.bfs.admin.ch/bfs/de/home/dienstleistungen/datenverknuepfungen/fuer-dritte.assetdetail.17084398.html>

11.5 Annexe 5: Conservation des données sur le nuage

Des tiers ne peuvent pas stocker sur un nuage les données fournies dans le cadre d'un projet d'appariement. Cette décision a été prise lors d'un échange avec le PFPDT et a fait l'objet d'une note (lien interne à l'OFS uniquement):  [Datenspeicherung in Cloud \(053.0-1/00008\)](#)

Un catalogue de critères a été élaboré pour décider des exceptions (lien interne à l'OFS uniquement):

 [SpeicherungGeteilteUmgebung_D_final](#)