Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral de l'intérieur DFI

Office fédéral de la santé publique OFSP
Unité de direction Assurance maladie et accidents

Règlement de traitement de la protection des données BAGSAN

Classification *	Aucune
Statut **	Approuvé
Nom du projet	Statistique de l'OFSP sur la base de données anonymisées des assurés (BAGSAN)
Mandant	Oliver Peters, vice-directeur de l'OFSP, responsable de l'unité de direction Assurance maladie et accidents (AMalA)
Maître du fichier (office, UA)	Office fédéral de la santé publique (OFSP), unité de direction Assurance maladie et accidents (AMalA)
Maître des données	Oliver Peters
Auteur	OFSP / AMalA / section Gestion des données et statistique (DMS)
Responsable d'application	OFSP / AMalA / DMS
CPDO	Federica Liechti
Traitement	OFSP / AMalA / DMS
Contrôle	Daniel Megert, DSIO
Version	1.0 *(n.d.t : traduite de la version originale allemande)*

* INTERNE, CONFIDENTIEL, SECRET
** En cours d'élaboration, en cours de vérification, terminé/approuvé

Suivi des modifications, contrôle, approbation

Version	Date	Description, remarque	Nom
0.1	02.08.2015	Création, transfert du règlement de traitement interne de l'OFSP	OFSP / AMalA / DMS
0.2	17.08.2015	Adaptation, transfert du règlement de traitement interne de l'OFSP	OFSP / AMalA / DMS
0.3	19.08.2015	Contrôle	OFSP DSIO
1.0	24.08.2015	Libération	Oliver Peters, vice-directeur, responsable de l'unité de direction Assurance maladie et accidents (AMalA)

Table des matières

1 Généralités 5

1.1 Bases du règlement de traitement 5
1.2 But du document 5

2 Règlement de traitement 5

2.1 Généralités 5
2.1.1 Nom et adresse de l'organe fédéral responsable 5
2.1.2 Nom et dénomination complète du fichier 6
2.1.3 Bases légales, généralités 6
2.1.4 Bases légales, BAGSAN 6
2.1.5 Bases légales, protection des données 7
2.1.6 But du fichier 7
2.1.7 Contexte 7
2.1.8 Catégories de données traitées 8

2.2 Documentation des unités administratives concernées par le système 9
2.2.1 Vue d'ensemble du système 9
2.2.2 Sous-systèmes 9
2.2.3 Description des interfaces 10
2.2.4 Délimitation 10
2.2.5 Organe responsable de la protection et de la sécurité des données 11
2.2.6 Organigramme de l'organe exploitant le système 11
2.2.7 Responsabilités 13

2.3 Liste des documents relatifs à la planification, à la réalisation et à l'exploitation du fichier 13
2.4 Déclaration du fichier au PFPDT 13
2.5 Processus 14
2.6 Procédure de contrôle, en particulier les mesures techniques et organisationnelles 15
2.6.1 Contrôle des accès 15
2.6.2 Contrôle des supports de données 15
2.6.3 Contrôle du transport 15
2.6.4 Contrôle de la communication des données 15
2.6.5 Contrôle du stockage des données 16
2.6.6 Contrôle des utilisateurs 16
2.6.7 Contrôle des droits d'accès 16
2.6.8 Contrôle de l'enregistrement des données 16

2.7 Contrôle des droits d'accès 17
2.7.1 Champs de données et unités administratives qui y ont accès 17
2.7.2 Nature et étendue de l'accès des utilisateurs 17
2.7.3 Droits d'accès 18

2.8 Procédures de traitement des données 18
2.8.1 Rectification 18
2.8.2 Blocage 18
2.8.3 Anonymisation 18
2.8.4 Sauvegarde 20
2.8.5 Conservation et archivage 20
2.8.6 Destruction 20

2.9 Configuration des moyens informatiques 21
2.10 Procédure d'exercice du droit d'accès 21
2.11 Déclaration du fichier 22

2.12 Liste des documents 22
2.13 Abréviations 23
2.14 Définitions 24

1 Généralités

1.1 Bases du règlement de traitement

Dans le cadre des projets informatiques de l'administration fédérale, le concept de sécurité de l'information et de protection des données (SIPD) constitue la base du règlement de traitement. Le maître d'un fichier automatisé élabore un règlement de traitement lorsque le fichier (cf. art. 21 de l'ordonnance relative à la loi fédérale sur la protection des données, OLPD ; RS 235.11) :

- contient des données personnelles sensibles ou des profils de la personnalité ;
- est utilisé par plusieurs organes fédéraux ;
- est accessible aux cantons, à des autorités étrangères, à des organisations internationales ou à des personnes privées, ou
- est connecté à d'autres fichiers.

Un fichier au sens de l'art. 3, let. g, de la loi fédérale sur la protection des données (LPD) est défini comme suit :
fichier, tout ensemble de données personnelles dont la structure permet de rechercher les données par personne concernée.

Le règlement de traitement doit garantir la transparence nécessaire dans le cadre du développement et de l'adaptation du système, ainsi que du traitement informatique de données personnelles. Il doit être mis à jour régulièrement (environ tous les trois ans).

L'art. 21 en relation avec l'art. 16 OLPD précise le contenu minimal du règlement de traitement.

Le projet suit la structure des contenus du Préposé fédéral à la protection des données et à la transparence (PFPDT). Il tient aussi compte des contenus du modèle de l'Unité de pilotage informatique de la Confédération (UPIC).

1.2 But du document

Le règlement de traitement décrit en particulier l'organisation interne de l'organe fédéral responsable, de même que les procédures de traitement et de contrôle des données. Il énumère tous les documents relatifs à la planification, à la réalisation et à l'exploitation du fichier. Il vise avant tout à instaurer une transparence optimale du traitement automatisé de données personnelles et de mesures permettant d'identifier et d'évaluer des risques éventuels pour la protection des données.

2 Règlement de traitement

2.1 Généralités

2.1.1 Nom et adresse de l'organe fédéral responsable

Office fédéral de la santé publique OFSP
Schwarzenburgstrasse 157
3003 Berne

2.1.2 Nom et dénomination complète du fichier

BAGSAN (Statistique de l'OFSP sur la base de données anonymisées des assurés)
(n.d.t : fichier répertorié auprès du PFPDT sous le nom BAGSAN (BAG Statistik auf Basis von anonymisierten Versichertendaten))

2.1.3 Bases légales, généralités

Les organes fédéraux sont habilités à traiter des données personnelles pour autant qu'une base légale le permette (art. 17 LPD).

Des données sensibles et des profils de la personnalité ne peuvent être traités que si une loi au sens formel le prévoit expressément ou lorsqu'exceptionnellement :

- une tâche clairement définie dans une loi au sens formel l'exige ;
- le Conseil fédéral l'autorise dans le cas particulier, parce que les droits de la personne concernée ne sont pas menacés ; ou
- la personne concernée a donné son consentement dans le cas particulier, ou a rendu ses données accessibles et n'en a pas expressément interdit le traitement.

Lorsque le traitement de données personnelles a été délégué à des tiers sur la base d'une convention (p. ex. un contrat de sous-traitance) ou de la loi, les conditions qui suivent doivent être remplies en vertu de l'art. 10*a*, al. 1, LPD :

- seuls les traitements que le mandant (office, unité administrative) serait en droit d'effectuer lui-même sont effectués, et
- aucune obligation légale ou contractuelle de garder le secret ne l'interdit.

Le mandant (ou l'organe fédéral responsable) doit en particulier s'assurer que le tiers garantisse la sécurité des données (art. 10*a*, al. 2, LPD).

2.1.4 Bases légales, BAGSAN

Dans le cadre de la surveillance de l'application de la loi sur l'assurance-maladie (LAMal), les assureurs sont tenus de fournir à l'autorité de surveillance, à l'organe de révision externe ou aux personnes mandatées par l'autorité de surveillance tous les renseignements et documents nécessaires à l'exécution de la surveillance de l'assurance-maladie sociale (art. 35, al. 1, de la loi sur la surveillance de l'assurance-maladie, LSAMal). Ils sont tenus de fournir chaque année à l'autorité de surveillance des indications sur les données liées à leur activité en matière d'assurance-maladie sociale. L'autorité de surveillance peut leur demander ces indications plusieurs fois par an (art. 35, al. 2, LSAMal).

Le but du fichier est précisé à l'art. 28, al. 1, de l'ordonnance sur l'assurance-maladie (OAMal).
L'art. 84*a*, al. 1, let. a, LAMal permet aux assureurs de communiquer des données personnelles, y compris des données sensibles et des profils de la personnalité, à l'OFSP, qui est l'autorité de surveillance. En vertu de l'art. 84 LAMal, celui-ci peut traiter ou faire traiter ces données personnelles, y compris les données sensibles et les profils de la personnalité, qui lui sont nécessaires pour accomplir les tâches que l'art. 34 LSAMal lui assigne. Le Conseil fédéral a fixé la nature et le volume des données à fournir par assuré à l'art. 28, al. 3, OAMal. L'OFSP est responsable de garantir l'anonymat des

assurés dans le cadre de l'exploitation des données (art. 28, al. 5, OAMal).

2.1.5 Bases légales, protection des données

L'OFSP, en tant que maître du fichier (art. 3, let. i, LPD), est tenu d'informer le fournisseur sur le maître des données, les buts du traitement et, le cas échéant (s'il est prévu de communiquer les données), les catégories de destinataires des données. Le fournisseur doit pouvoir reconnaître la finalité de l'utilisation des données (adéquation).

L'OFSP met en œuvre les directives sur les exigences minimales qu'un système de gestion de la protection des données doit remplir et qui sont applicables pour les fichiers. Le traitement des données doit se conformer au principe de la proportionnalité (art. 4, al. 2, LPD).

2.1.6 But du fichier

Le fichier BAGSAN constitue la base de l'évaluation au sens des art. 28, 28*b* et 32 OAMal et 61 OSAMal.

Les données qui doivent être transmises par les assureurs en vertu de l'art. 35, al. 2, LSAMal et qui sont collectées dans le cadre du présent fichier permettent à l'OFSP d'exercer la surveillance des assureurs-maladie, de garantir l'égalité de traitement entre assurés, de les protéger contre les abus, d'examiner si les primes appliquées correspondent aux primes approuvées et de proposer des bases de décision en cas de révision nécessaire de la loi et de ses dispositions d'exécution.

2.1.7 Contexte

Dans le cadre de la surveillance de l'assurance-maladie (LAMal), les assureurs sont tenus de fournir à l'OFSP des indications sur les données liées à leur activité en matière d'assurance-maladie sociale (art. 35, al. 2, LSAMal). L'art. 28, al. 3, OAMal règle les modalités de la collecte de données, notamment les données par assuré. L'art. 28, al. 1, OAMal définit les buts pour lesquels les données sont collectées tandis que l'art. 28, al. 5 exige la garantie de l'anonymat des assurés lors de l'exploitation des données. En vertu de l'art. 28, al. 4, OAMal, les assureurs doivent fournir les données par voie électronique.

L'OFSP collecte des données individuelles pour des évaluations qui nécessitent une granularité à cette échelle c.a.d. qui ne peuvent pas être réalisées avec des données agrégées (selon le principe de proportionnalité).

Depuis 2014, l'OFSP collecte les données individuelles de manière anonymisée auprès des assureurs en vertu de l'art. 28, al. 4, OAMal ; il n'est donc pas possible d'identifier les personnes concernées (assurés). Les données individuelles collectées de façon décentralisée (auprès des assureurs LAMal) sont traitées dans le système BAGSAN et mises à la disposition des utilisateurs autorisés par l'OFSP de manière ciblée et adaptée à l'utilisateur. À noter que ces données sont traitées et utilisées à des fins d'analyses statistiques uniquement ; aucun travail ne porte sur les données d'assurés en particulier.

Les données anonymisées du fichier BAGSAN ne sont pas des données personnelles au sens de l'art. 3, let. a, LPD, car un lien avec une personne n'est pas possible ou tout au moins pas possible sans une charge de travail disproportionnée. L'OFSP veille, par le biais de mesures, à ce que le risque résiduel d'une réidentification (indirecte) puisse être exclu dans une large mesure lors du traitement. De plus, il a la responsabilité de préserver l'anonymat des assurés lors de l'exploitation des données et prend des mesures techniques et de procédure en conséquence.

2.1.8 Catégories de données traitées

La présente base de données de traitement comprend des données sur des personnes morales (assureurs) et des données anonymisées (données individuelles sans possibilité d'identifier les assurés).

BAGSAN permet de collecter, à l'échelle des données individuelles, des données sociodémographiques ainsi que des indications sur les primes et les coûts (AOS) en application de l'art. 28 OAMal. Un code de liaison anonyme est recueilli pour pouvoir calculer les coûts d'un assuré sur plus d'une année (mais sur cinq ans au maximum).

Aucune donnée sensible n'est traitée dans le présent fichier. La durée de traitement des livraisons est limitée à cinq ans. Cela correspond au délai fixé pour la présentation des pièces comptables AOS par les assurés, ce qui permet de calculer les coûts totaux par assuré en fonction de l'année de traitement.

Les données suivantes sont traitées :

Contenu	Type de données personnelles
<u>Assureurs :</u> N° OFSP (n° de caisse)	Données personnelles juridiques
<u>Données sociodémographiques à l'échelle des données individuelles :</u> Âge Sexe District Région Medstat Code de liaison anonyme	Données individuelles anonymisées
<u>Primes et coûts (AOS) à l'échelle des données individuelles :</u> Période de couverture, motif (catégorie) d'entrée et de sortie Classe de risque (classification selon compensation des risques) Assureurs Assurance o Prime o Région de prime o Modèle o Franchise o Couverture accidents incluse Primes payées (total) pour la période de couverture Coûts bruts AOS (total) pour la période de couverture Participation aux coûts AOS (total) pour la période de couverture	Données individuelles anonymisées

Tableau 1 : Liste des données

Remarque : modifications apportées aux caractéristiques depuis le premier relevé en 2014 :

- Pour les exercices 2013 et 2014, les relevés ont porté sur la commune et non sur le district pour le nouveau calcul des régions de primes. Une procédure appropriée a permis de garantir que les données utilisées pour l'évaluation ne permettaient aucune réidentification indirecte. À partir de l'exercice 2015, l'indication du district est transmise en lieu et place de la commune.

2.2 Documentation des unités administratives concernées par le système

2.2.1 Vue d'ensemble du système

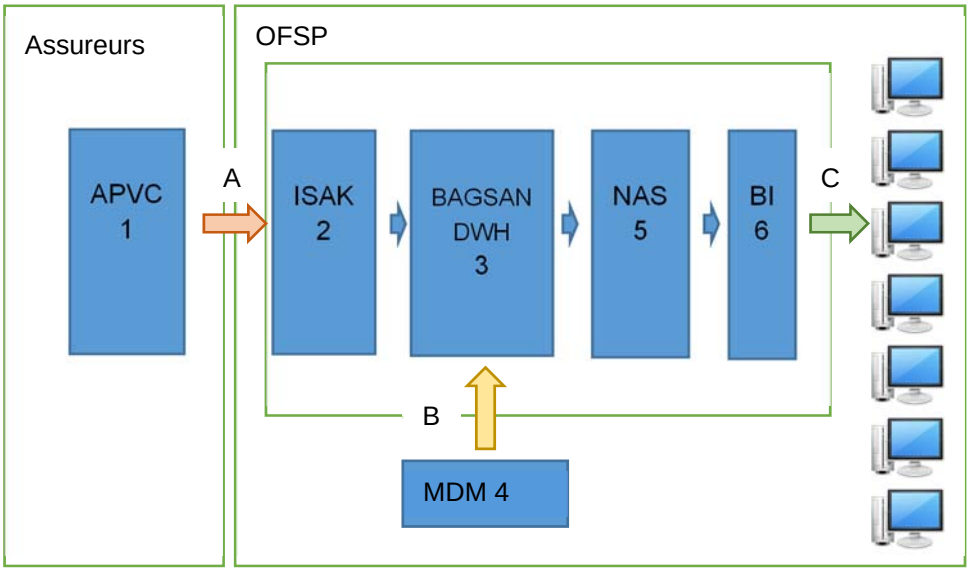

Figure 1 : Vue d'ensemble du système BAGSAN et de ses sous-systèmes.

2.2.2 Sous-systèmes

Le système se compose de six sous-systèmes :

Nº	Sigle	Désignation	Fonction dans le cadre de BAGSAN
1	APVC	Programme d'anonymisation, de plausibilisation et de cryptage	Logiciel de collecte décentralisée par les assureurs. Les données individuelles sont anonymisées sur place (chez les assureurs)
2	ISAK	Système d'information de la surveillance de l'assurance maladie	Transport des données et workflow
3	BAGSAN-DWH	Base de données de traitement BAGSAN	Extraction, transformation, traitement et stockage centralisé des données
4	MDM	Master Data Management	Base de données qui fournit les données de base nécessaires pour l'année sous revue (ne contient pas de données individuelles)
5	NAS	Network Storage	Stockage des données d'analyse (anonymisées)
6	BI	Plate-forme statistique BAGSAN	Mise à disposition des données contrôlée et adaptée aux utilisateurs par le biais d'une plate-forme de Business Intelligence

Tableau 2 : Description des sous-systèmes BAGSAN.

L'OFSP envoie chaque année le logiciel APVC (1) aux assureurs pour la saisie décentralisée des données individuelles. Les données sont anonymisées sur place (chez les assureurs) et préparées sous forme de paquets cryptés. La transmission de ces paquets à l'OFSP s'effectue par le biais de la plate-forme ISAK (2), qui permet le transport et la réception des données. Les paquets cryptés parviennent dans la base de données de traitement BAGSAN (3) au sein du réseau sécurisé de la Confédération. En plus des données individuelles anonymisées, (3) permet de collecter des données de base (p. ex., liste des tarifs de primes) et de comparaison (p. ex., table des portefeuilles d'assurance par canton ou par assureur ; il s'agit exclusivement de données agrégées, issues notamment de la statistique LAMal) tirées du MDM. Dans le cadre de (3), les données sont déchiffrées, validées et traitées selon un processus bien défini, déposées dans un entrepôt de données (Datawarehouse, DWH) et décomposées en sous-ensembles non combinables, si bien qu'une réidentification indirecte est impossible, même si les données sont disponibles plusieurs années. Les données traitées sont transportées sur un Network Storage physiquement séparé et protégé (5) et servent de base pour les évaluations statistiques sur la plate-forme statistique BAGSAN, qui se trouve aussi dans le réseau interne de la Confédération (6).

Les données validées par (6) pour exploitation sont vérifiées par un spécialiste de la protection des données selon un processus bien défini. Seuls les collaborateurs de l'OFSP enregistrés et autorisés ont accès aux rapports de la plate-forme statistique (6).

2.2.3 Description des interfaces

La gestion des données BAGSAN comprend trois interfaces avec des systèmes périphériques :

N°	Fonction
A	Interface avec les assureurs qui déposent sur ISAK les données individuelles anonymisées et cryptées pour l'OFSP, traitées avec APVC. Le dépôt s'appuie sur une transmission cryptée. Les données parviennent dans la base de données de traitement (3) par le biais d'un processus sécurisé bien défini et les données cryptées déposées sur ISAK sont supprimées.
B	Interface avec le MDM, à partir duquel le système BAGSAN se procure les données de base et de comparaison. Le transfert des données s'effectue au sein du réseau de la Confédération. Il n'y a aucun échange de données individuelles.
C	Interface avec des collaborateurs de l'OFSP autorisés qui utilisent les données BAGSAN pour des évaluations statistiques. L'accès s'effectue par le biais de la plate-forme statistique BI, qui se trouve aussi dans le réseau interne de la Confédération.

Tableau 3 : Interfaces du système BAGSAN.

2.2.4 Délimitation

Le document est soumis aux délimitations suivantes :

- Les considérations portent en premier lieu sur les aspects pertinents en matière de protection des données, en particulier la protection des données individuelles anonymisées au sein du système BAGSAN (notamment les sous-systèmes DWH [3], NAS [5] et BI [6] selon la figure 1).

- Le présent règlement de traitement décrit les faits sous un angle opérationnel. Les aspects déterminants en matière de TIC sont décrits dans le concept SIPD de l'OFSP.

2.2.5 Organe responsable de la protection et de la sécurité des données

Domaine de responsabilité	Responsable (désignation du rôle)
Conseiller à la protection des données	Conseiller à la protection des données OFSP (CPDO)
Responsable sécurité informatique, conseil (sécurité des données)	Délégué à la sécurité informatique OFSP (DSIO)
Responsable d'application	OFSP / AMalA / section Gestion des données et statistique (DMS)
Responsable de la collecte de données	OFSP / AMalA / DMS
RSIPD	OFSP / AMalA / DMS
Responsable des processus	OFSP / AMalA / responsable de la section DMS

L'organe responsable de la protection et de la sécurité des données est, en tant que maître du fichier, l'OFSP (art. 3, let. i, LPD : maître du fichier, *la personne privée ou l'organe fédéral qui décide du but et du contenu du fichier*).

Au sein de l'office, les unités de direction sont responsables des données qui relèvent de leur domaine de compétences.

Les conseils en matière de protection des données sont assurés par le conseiller à la protection des données (CPDO). Sa tâche est de soutenir et d'informer les utilisateurs ainsi que de participer à l'application des dispositions en matière de protection des données. Il accomplit ses tâches en collaboration avec le délégué à la sécurité informatique de l'office.

Les conseils donnés aux utilisateurs de la base de données de traitement BAGSAN en matière de sécurité des données ou de protection technique des données sont assurés par le délégué à la sécurité informatique (DSIO). Il calcule et évalue les risques liés à la sécurité informatique dans l'office, qu'il soutient quant à la mise en œuvre, au respect et à l'efficacité des mesures de sécurité informatique.

2.2.6 Organigramme de l'organe exploitant le système

L'organigramme ci-dessous (figure 2) montre la structure hiérarchique de l'OFSP, avec la section DMS qui exploite le système (en bleu) au sein de la division Surveillance de l'assurance (en rouge).

D'une part, le nombre de collaborateurs qui travaillent dans le processus de traitement s'élève à quelques personnes de la section Gestion des données et statistique. D'autre part, l'exploitation des données se limite aux collaborateurs de l'OFSP autorisés qui sont enregistrés sur la plate-forme d'évaluation (6).

Figure 2 : Organigramme OFSP

2.2.7 Responsabilités

Qui	Nom
Exploitant du système	Fournisseur de prestations interne à la Confédération (OFIT)
Fournisseur de prestations	Fournisseur de prestations interne à la Confédération, fournisseur du logiciel statistique
Interlocuteur auprès du fournisseur de prestations (FP)	Collaborateur OFIT
DSID	Roland Gafner (OFIT)
DSIO	Daniel Megert (OFSP)
CPDO	Federica Liechti (OFSP)
Maître des données	Office fédéral de la santé publique, division Assurance maladie et accidents (AMalA)
Responsable d'application	Office fédéral de la santé publique, division Assurance maladie et accidents, section Gestion des données et statistique
Cercle d'utilisateurs	Office fédéral de la santé publique

Tableau 4 : Responsabilités

2.3 Liste des documents relatifs à la planification, à la réalisation et à l'exploitation du fichier

Les documents relatifs à la planification, à la réalisation et à l'exploitation des systèmes sont conservés au sein de la section DMS de la division AMalA.

2.4 Déclaration du fichier au PFPDT

Voir section 2.11

2.5 Processus

Les étapes du processus de traitement des données sont :

Nº	Brève description	Sous-système (cf. figure 1)
1	Préparation de la collecte de données (y c. traitement des données de base pour la collecte, actualisation APVC, si nécessaire mise à jour des mesures de sécurité et d'anonymisation)	APVC, MDM
2	Importation des données de base MDM dans BAGSAN-DWH	MDM, BAGSAN-DWH
3	Transport des données cryptées d'ISAK vers le serveur de traitement BAGSAN	ISAK, BAGSAN-DWH
4	Extraction y. c. déchiffrage, chargement et transformation (ETL) des données dans la base de données de traitement	BAGSAN-DWH
5	Validation formelle par assureur (par fourniture de données) Annonce de statut aux assureurs, si nécessaire concertation et nouvelle transmission de données	BAGSAN-DWH
6	Validation formelle de toutes les données (au-delà des assureurs, pour un relevé) Annonce de statut aux assureurs, si nécessaire concertation et nouvelle transmission de données	BAGSAN-DWH
7	Chargement des données transformées et formellement validées dans le datawarehouse	BAGSAN-DWH
8	Chargement des données de comparaison MDM (données de la statistique LAMal)	BAGSAN-DWH
9	Validation statistique au moyen des données de comparaison Annonce de statut aux assureurs, si nécessaire concertation et nouvelle transmission de données	BAGSAN-DWH
10	Libération des données validées du datawarehouse pour la suite du traitement	BAGSAN-DWH
11	Création des bases de données (décomposition des données du datawarehouse en sous-ensembles)	BAGSAN-DWH
12	Exécution de la fonction de représentativité	BAGSAN-DWH
13	Création des « views » en se fondant sur les bases de données (application de filtres et simplification en fonction du rapport)	BAGSAN-DWH
14	Chargement des « views » dans l'entrepôt du serveur d'évaluation	BAGSAN-DWH, NAS
15	Vérification (en termes de contenus et de protection des données) et validation des rapports	BI
16	Publication des rapports sur le serveur d'évaluation, mise à disposition adaptée aux utilisateurs	BI
17	Information des utilisateurs autorisés	BI

En plus des étapes du processus de traitement des données, il existe un déroulement réglementé qui précise comment les collaborateurs de l'OFSP ont accès aux données validées pour l'exploitation.

2.6 Procédure de contrôle, en particulier les mesures techniques et organisationnelles

Le système BAGSAN prévoit plusieurs procédures qui contribuent à la sécurité de la conservation des données :

- Avant la mise en service, les fonctions critiques et importantes du point de vue de la sécurité sont contrôlées par le fournisseur de prestations interne à la Confédération pour les services informatiques.
- Les mesures de sécurité et d'anonymisation sont vérifiées une nouvelle fois avant toute collecte et avant la validation du programme d'anonymisation APVC et actualisées le cas échéant.
- Le nombre d'utilisateurs du système de traitement BAGSAN se chiffre à quelques collaborateurs de la section Gestion des données et statistique. Le nombre de collaborateurs de l'OFSP ayant accès aux données validées pour exploitation via la plate-forme statistique BI est aussi limité. Les accès sont attribués de manière restrictive et uniquement en cas de besoin et nécessitent l'approbation du responsable de la section DMS.
- Il n'existe aucun accès à distance externe à l'infrastructure BAGSAN DWH (3).
- Les processus de traitement des données au sein de BAGSAN DWH (3) sont déclenchés et surveillés, mais pas modifiés par les collaborateurs BAGSAN.
- En plus des règles d'accès (restrictives), les processus de traitement déterminants sont enregistrés.

2.6.1 Contrôle des accès

Le bâtiment de l'OFSP est protégé par des contrôles d'accès personnels (loge) et techniques (badges). Les collaborateurs de l'OFSP sont en outre tenus de chercher les visiteurs à l'accueil et de les raccompagner à la sortie.

Les documents sur papier se trouvent dans des armoires fermées à clé.

2.6.2 Contrôle des supports de données

L'ensemble de l'infrastructure informatique du système BAGSAN se trouve dans le centre de calcul sécurisé du fournisseur de prestations interne à la Confédération pour les services informatiques. Aucune donnée productive n'est transférée ou utilisée dans les environnements de test dans le cadre de BAGSAN. Les environnements de test se servent de fichiers randomisés et anonymisés.

2.6.3 Contrôle du transport

Les transports de données vers les interfaces du système BAGSAN (figure 1) sont entièrement cryptés.

2.6.4 Contrôle de la communication des données

Les données du fichier BAGSAN sont validées pour exploitation par le biais de la plate-forme statistique BI (sous-système 6, cf. figure 1). Les collaborateurs sont sensibilisés à l'obligation de traiter les données du système et donc de les communiquer en respectant la voie et les processus officiels. La plate-forme statistique est la seule instance de communication.

2.6.5 Contrôle du stockage des données

Les données sont sécurisées de manière cryptée. L'accès au serveur est réglementé dans le SLA (Service Level Agreement) avec le fournisseur de prestations interne à la Confédération pour les services informatiques.

Les supports de données se trouvent dans des locaux protégés. La connexion aux ordinateurs clients, avec accès aux supports de données, s'effectue au moyen d'une authentification à deux facteurs conformément aux exigences de protection de base des TIC dans l'administration fédérale.

2.6.6 Contrôle des utilisateurs

La connexion au poste de travail est protégée par une authentification à deux facteurs. La connexion aux deux serveurs BAGSAN DWH et BI (cf. figure 1) requiert une identification supplémentaire avec nom d'utilisateur personnel et mot de passe.

Il n'existe pas d'accès à distance au système BAGSAN en dehors de l'équipement normal du poste de travail.

L'accès administratif à BAGSAN DWH est soumis à un processus de validation où le DSIO doit approuver une demande du responsable de la section DMS.

2.6.7 Contrôle des droits d'accès

L'accès des utilisateurs est limité en fonction des rôles (cf. section 2.7.1). Chaque utilisateur dispose d'un compte utilisateur personnel. Le cercle des utilisateurs ayant accès au système BAGSAN (cf. figure 1) se limite aux collaborateurs de la section DMS pour le traitement, aux collaborateurs de l'OFSP autorisés et authentifiés pour l'exploitation des données. La connexion à l'ordinateur client de la Confédération s'effectue au moyen d'une authentification à deux facteurs.

Il n'y a pas d'accès aux systèmes de traitement et d'évaluation pour les prestataires externes. Le support et la maintenance sont réalisés sur place, le cas échéant sous la surveillance de la section Gestion des données et statistique ou du fournisseur de prestations interne à la Confédération pour les services informatiques.

2.6.8 Contrôle de l'enregistrement des données

Cette section décrit le contrôle de l'enregistrement des données (personne responsable et procédure).

a. Compétence

   Dans le système BAGSAN, les données sont exclusivement traitées par des collaborateurs BAGSAN (section DMS). Le traitement des données s'effectue par le biais de programmes prédéfinis et il est enregistré (p. ex., temps, utilisateur, activité, objet).

   Les connexions aux différents sous-systèmes BAGSAN sont historisées et régulièrement contrôlées.

b. Mise en œuvre du contrôle de l'enregistrement des données : validation, correction et historisation

L'enregistrement des données est contrôlé en plusieurs étapes.

- Certains contrôles sont déjà effectués par le biais d'APVC avant la réception des données. Les jeux de données ont la mention sans erreur ou avec erreurs (avec message d'erreur).
- Après la réception des données, il y a d'autres étapes de validation définies dans la documentation au sein de la base de données de traitement (BAGSAN DWH). Le cas échéant, la transmission de nouvelles données est demandée aux assureurs.
- Les données validées pour exploitation ne contiennent que les jeux de données qui satisfont aux critères définis.

2.7 Contrôle des droits d'accès

2.7.1 Champs de données et unités administratives qui y ont accès

Les acteurs bénéficiant de droits d'accès aux données se répartissent en trois catégories : les assureurs, les collaborateurs BAGSAN (collaborateurs de la section Gestion des données et statistique de l'OFSP) et les collaborateurs de l'OFSP. Ils se distinguent en fonction du sous-système auquel ils peuvent accéder (figure 1). Les assureurs fournissent les données, mais n'ont pas accès aux données déposées sur les serveurs de traitement de l'OFSP. Les collaborateurs de l'OFSP autorisés n'ont accès qu'aux données validées pour exploitation qui sont passées par les sous-systèmes BAGSAN (ISAK, BAGSAN DWH, NAS et BI). Les collaborateurs BAGSAN sont chargés du traitement des données dans le système BAGSAN et ont par conséquent accès de manière sélective, en fonction de leur tâche, aux sous-systèmes ISAK, BAGSAN DWH, NAS ou BI.

2.7.2 Nature et étendue de l'accès des utilisateurs

Le tableau 5 résume les droits d'accès de ces trois acteurs (assureurs, collaborateurs BAGSAN et collaborateurs de l'OFSP). Les descriptions plus précises des droits d'accès figurent dans les règlements de traitement et les manuels d'exploitation correspondants.

Élément d'information / Rôle	APVC Input	ISAK Input	DWH	MDM	NAS	BI Output
	1	2	3	4	5	6
Assureurs	x	x				
Collaborateurs BAGSAN*		r	x	r	x	x
Collaborateurs de l'OFSP				r		r

Tableau 5 : Rôles et droits d'accès. Légende : x = accès intégral, r = read only, vide = pas d'accès.

*Les règles d'accès de la catégorie « collaborateurs BAGSAN » sont présentées ici de manière résumée. Les règles d'accès détaillées permettent notamment de garantir qu'un collaborateur ne peut pas exécuter seul toutes les étapes du processus de traitement.

2.7.3 Droits d'accès

Le chef de la section DMS a la responsabilité des droits d'accès. De plus, une autorisation du DSIO pour les droits d'accès au sous-système de traitement est nécessaire. L'activation est effectuée par le fournisseur de prestations interne à la Confédération pour les services informatiques.

2.8 Procédures de traitement des données

Comme les données sont anonymisées, l'OFSP ne dispose pas de procédure de destruction, de blocage ni de droit de rectification concernant les données individuelles. Les assureurs (personnes morales) peuvent s'assurer de la rectification de leurs données en transmettant de nouvelles données.

2.8.1 Rectification

Les modifications sont annoncées à la section spécialisée. La mise en œuvre est effectuée par le responsable technique en collaboration avec le responsable d'application. Les modifications de la définition des rôles doivent être validées au préalable par le responsable de la section et, si nécessaire, par le DSIO. L'attribution ou le retrait de droits d'accès sont consignés par écrit (au moins par courriel).

2.8.2 Blocage

Il n'est pas prévu de bloquer des jeux de données. Ils sont vérifiés sur le plan statistique, et le cas échéant rectifiés et historisés selon un processus de validation bien défini.

2.8.3 Anonymisation

La procédure d'anonymisation est notamment mise en œuvre aux points suivants :

Collecte :

- Le programme d'anonymisation APVC (sous-système 1, figure 1) transforme le numéro AVS, seule donnée qui puisse servir à une réidentification directe, en un *code-hash* complètement anonyme pour l'OFSP. Un algorithme SHA-2 est utilisé pour la transformation. Le code secret (SALT) est exclusivement conservé par l'éditeur du logiciel APVC et n'est pas accessible à l'OFSP. Celui-ci ne peut ni reconstruire les numéros AVS provenant d'une transmission de données, ni répliquer le processus de hachage.
- APVC simplifie les caractéristiques démographiques qui pourraient servir à une identification personnelle indirecte. L'indication du numéro postal d'acheminement est par exemple remplacée par les régions MedStat (selon les nomenclatures de l'OFS). Les transformations de données par APVC permettent d'anonymiser les données que les assureurs fournissent à l'OFSP afin d'éviter une réidentification. L'OFSP vérifie l'adéquation de ces transformations avant la collecte de données et la libération du logiciel APVC.
- Pour le développement, l'OFSP dispose d'une version d'APVC avec un code secret modifié (SALT). Cela lui permet de tester APVC sans prendre de risques sur le plan de la sécurité. Seules des données anonymisées et randomisées sont utilisées pour le développement.

Traitement des données :

- Les codes de liaison fournis, c'est-à-dire les *codes-hash* des numéros AVS, sont remplacés par un code de liaison anonyme interne à l'OFSP pour qu'ils ne soient pas disponibles dans le datawarehouse.

- Pour le traitement des données, des mesures supplémentaires sont prises dans le data-warehouse afin d'éviter les risques éventuels de réidentification liés au stockage de données sur plusieurs années. Les codes de liaison anonymes, par exemple, sont conservés dans des tables protégées et séparées. Les processus et accès sont aussi enregistrés si nécessaire.
- Dans la base de données de traitement, les droits sont définis à l'aide de rôles, si bien que le déchiffrage, le chargement des données, etc. sont effectués de manière sélective par différents collaborateurs. Il est impossible qu'un collaborateur exécute seul toutes les étapes du processus de traitement.
- Avant que les données ne soient disponibles pour exploitation, d'autres transformations sont effectuées dans la base de données de traitement (sous-système 3, figure 1) et sur la plate-forme statistique (sous-système 6, figure 1) pour que les données soient mises à disposition en fonction du contexte (donc en fonction des rapports et des droits d'accès des utilisateurs). Cette approche permet de garantir que seuls sont disponibles les caractéristiques et le niveau d'agrégation nécessaires aux buts de l'évaluation. Les données sont traitées individuellement conformément aux droits d'accès des utilisateurs. Les modalités du traitement sont vérifiées par un spécialiste de la protection des données. Il existe un processus de validation spécifique pour la création ou la mutation des rapports.

Exploitation des données :

- Le code de liaison anonyme interne à l'OFSP est remplacé par des numéros séquentiels aléatoires pour l'établissement des rapports. De plus, l'ordre des jeux de données est randomisé. Les données ne peuvent donc pas être mises en relation.
- Lors de l'établissement des rapports sur la plate-forme statistique, accessible aux collaborateurs de l'OFSP autorisés, un contrôle de qualité est effectué par un collaborateur spécialiste de la protection des données avant leur validation. Ce contrôle garantit que les données des rapports sont complètement anonymes concernant les assurés.

L’exemple suivant illustre la transformation d’un enregistrement :

Il montre comment un enregistrement traité par l’assureur (tableau A) pour une personne fictive ayant le numéro AVS « 7569513811202 » est transformé en un enregistrement ensuite accessible à l’OFSP pour le traitement (tableau B).

Tableau A : Jeu de données illustratif (input). Données traitées par l’assureur pour la transmission.

Code de liaison	Caractéristiques démographiques				Fait
Numéro AVS	Commune	Année de naissance	Sexe	Franchise	Coûts bruts
*7569513811202**	*606**	1983	F	300	20000.35

*** non consultable par l’OFSP**

➔ Transformation par APVC

Tableau B : Jeu de données illustratif (output) du logiciel APVC. Données traitées par les collaborateurs BAGSAN autorisés après déchiffrage.

Code de liaison	Caractéristiques démographiques				Fait
Code de liaison anonyme	District	Année de naissance	Sexe	Franchise	Coûts bruts
lho+Bx9a8Bs0eSlYAc9919GqQ5VN/7FElcXlKPgj9EXh0CAWw73b31KzluwZEYS+	*2573*	1983	F	300	20000.35

Comme l’illustre l’exemple, le numéro AVS, en soi anonyme mais clairement attribué à une personne physique dans le registre correspondant (chez l’assureur), est transformé en code de liaison anonyme « lho+Bx9a8Bs0eSlYAc9919GqQ5VN/7FElcXlKPgj9EXh0CAWw73b31KzluwZEYS+ ». La transformation du numéro AVS en code de liaison anonyme ne peut pas être reconstituée par l’OFSP. En d’autres termes, l’OFSP n’est pas en possession de la clé de transformation inverse qui lui permettrait de déduire « 7569513811202 » à partir de « lho+Bx9a8Bs0eSlY… ». De même, il ne possède pas les éléments nécessaires pour répliquer la transformation qui permettrait, à partir de « 7569513811202 », de générer le code de liaison « lho+Bx9a8Bs0eSlY... ».

2.8.4 Sauvegarde

L’infrastructure informatique du système BAGSAN est sauvegardée auprès d’un fournisseur de prestations interne à la Confédération. Les processus de sauvegarde sont coordonnés avec lui et figurent obligatoirement dans le manuel d’exploitation interne.

2.8.5 Conservation et archivage

Le système BAGSAN exploite les données des cinq dernières années de référence. Les données transmises sont conservées pendant dix ans de manière cryptée sur le serveur BAGSAN dans un emplacement séparé et sauvegardées par le biais du processus normal d’exploitation.

2.8.6 Destruction

Les données de la base de données de traitement sont détruites après dix ans pour autant qu’elles ne

soient pas transmises aux Archives fédérales à des fins d'archivage au sens de la loi fédérale sur l'archivage (RS 152.1). À cette fin, la base de données de traitement est saisie dans le système de classement (plan d'enregistrement) de l'OFSP. Les Archives fédérales décident avec l'OFSP quelles données sont archivées pour documenter les actions déterminantes de l'État. L'OFSP évalue la valeur archivistique des données selon des critères juridiques et administratifs. Les Archives fédérales se fondent sur des aspects historiques et sociaux. Elles prennent en charge les données présentant une valeur archivistique et les archivent à long terme sous forme numérique.

2.9 Configuration des moyens informatiques

La configuration et l'exploitation des moyens informatiques hébergés (infrastructure et hébergement du matériel informatique) relèvent de la compétence du fournisseur de prestations interne à la Confédération.

La configuration des applications relève de la compétence du responsable d'application (collaborateur BAGSAN, section DMS). Il s'agit de la configuration des *shares*, des structures de fichiers, du logiciel de traitement de données et des objets de données résultant du traitement de données. Ces configurations sont documentées dans les manuels d'exploitation internes.

Les droits d'accès sont attribués par le responsable d'application après validation par le responsable de la section DMS et, le cas échéant, par le DSIO. Ils sont régulièrement contrôlés.

2.10 Procédure d'exercice du droit d'accès

Comme le fichier est déjà anonymisé lors de la collecte s'agissant des assurés (l'OFSP ne peut générer aucun lien direct avec une personne), le droit d'accès (art. 8 LPD) n'est pas applicable en ce qui concerne les données individuelles. Par conséquent, aucune procédure n'est définie en matière de droit d'accès.

Les assureurs LAMal concernés peuvent exercer leur droit de consultation (droit d'accès) en faisant parvenir leur question par écrit à l'adresse suivante :

Office fédéral de la santé publique
Unité de direction Assurance maladie et accidents
Division Surveillance de l'assurance
Section Gestion des données et statistique
Schwarzenburgstrasse 157
3003 Berne

Courriel : KUV-DMS@bag.admin.ch

2.11 Déclaration du fichier

Le fichier « base de données de traitement BAGSAN » (statistique de l'OFSP sur la base des données anonymisées des assurés)[1] a été déclaré le 29 avril 2016 au PFPDT. La description du fichier peut être consultée sur le lien suivant :

https://www.datareg.admin.ch/search/ResultDetail.aspx?RegNr=201600061

2.12 Liste des documents

Liste de tous les textes pertinents pour le fichier concerné (lois, ordonnances, directives, réglementations). Les documents sur la planification, la mise en œuvre et l'exploitation des systèmes sont conservés par la section Gestion des données et statistique.

Type de document	N°	Titre
Lois		Loi fédérale du 19 juin 1992 sur la protection des données (LPD ; RS 235.1)
		Loi fédérale du 17 décembre 2004 sur le principe de la transparence dans l'administration (loi sur la transparence, LTrans ; RS 152.3)
		Loi fédérale du 26 juin 1998 sur l'archivage (LAr ; RS 152.1)
		Loi fédérale du 18 mars 1994 sur l'assurance-maladie (LAMal ; RS 832.10)
		Loi fédérale du 26 septembre 2014 sur la surveillance de l'assurance-maladie sociale (loi sur la surveillance de l'assurance-maladie, LSAMal ; RS 832.12)
Ordonnances		Ordonnance du 9 décembre 2011 sur l'informatique et la télécommunication dans l'administration fédérale (ordonnance sur l'informatique dans l'administration fédérale, OIAF ; RS 172.010.58)
		Ordonnance du 14 juin 1993 relative à la loi fédérale sur la protection des données (OLPD ; RS 235.11)
		Ordonnance du 4 juillet 2007 concernant la protection des informations de la Confédération (ordonnance concernant la protection des informations, OPrI ; RS 510.411)
		Ordonnance du 26 octobre 2011 concernant la protection des données personnelles du personnel de la Confédération (RS 172.220.111.4)
		Ordonnance du 27 juin 1995 sur l'assurance-maladie (OAMal ; RS 832.102)
		Ordonnance du 18 novembre 2015 sur la surveillance de l'assurance-maladie sociale (ordonnance sur la surveillance de l'assurance-maladie, OSAMal ; RS 832.121)
		Ordonnance du 12 avril 1995 sur la compensation des risques dans l'assurance-maladie (OCoR ; RS 832.112.1)
		Ordonnance du 20 juin 2014 sur l'adaptation de structures tarifaires dans l'assurance-maladie (RS 832.102.5)
		Ordonnance du 12 septembre 2014 sur la correction des primes (RS 832.107.21)
		Ordonnance du DFI du 29 septembre 1995 sur les prestations dans l'assurance obligatoire des soins en cas de maladie (ordonnance sur les prestations de l'assurance des soins, OPAS ; RS 832.112.31)
		Ordonnance de l'OFSP du 25 août 2015 sur le montant du supplément de prime pour 2016 (RS 832.107.22)

[1] *n.d.t : fichier répertorié auprès du PFPDT sous le nom BAGSAN (BAG Statistik auf Basis von anonymisierten Versichertendaten*)

Type de document	N°	Titre
		Ordonnance de l'OFSP du 18 février 2016 sur le montant de la diminution de prime pour 2016 (RS 832.107.23)
		Ordonnance de l'OFSP du 18 février 2016 sur le montant du remboursement de primes pour 2016 (RS 832.107.24)
Directives		Voir annexe de l'ordonnance du 4 juillet 2007 concernant la protection des informations de la Confédération (ordonnance concernant la protection des informations, OPrI ; RS 510.411)
Guides		Document du PFPDT *Que doit donc contenir un règlement de traitement ?*
		Guide pour le traitement des données personnelles dans l'administration fédérale, PFPDT, 1er août 2009
		Guide pour l'élaboration des bases légales nécessaires pour exploiter un système de traitement automatisé de données personnelles, OFJ, 16 décembre 2010
		Guide relatif aux mesures techniques et organisationnelles de la protection des données, août 2015

2.13 Abréviations

Abréviation	Signification
Al.	Alinéa
Art.	Article
RA	Responsable d'application
OFSP	Office fédéral de la santé publique
BAGSAN	Statistique de l'OFSP sur la base de données anonymisées des assurés
BI	Business Intelligence (abréviation pour la plate-forme statistique BAGSAN)
OFIT	Office fédéral de l'informatique et de la télécommunication
Let.	Lettre
CPDO	Conseiller à la protection des données de l'UA (office, département)
LPD	Loi fédérale sur la protection des données (RS 235.1)
DWH	Data Warehouse (élément de la base de données de traitement BAGSAN)
DFI	Département fédéral de l'intérieur
PFPDT	Préposé fédéral à la protection des données et à la transparence
ETL	Extract, Transform, Load Process (élément de la base de données de traitement BAGSAN)
TIC	Technologies de l'information et de la communication dans l'administration fédérale
ISAK	Système d'information de la surveillance de l'assurance-maladie
UPIC	Unité de pilotage informatique de la Confédération
DSIO	Délégué à la sécurité informatique de l'UA
DSID	Délégué à la sécurité informatique du département
Concept SIPD	Concept de sécurité de l'information et de protection des données
RSIPD	Responsable de la sécurité de l'information et de la protection des données
LSAMal	Loi sur la surveillance de l'assurance-maladie
LAMal	Loi fédérale sur l'assurance-maladie
FP	Fournisseur de prestations

Abréviation	Signification
NAS	Network Attached Storage (lecteur réseau)
ODS	Operational Data Store (élément de la base de données de traitement BAGSAN)
UA	Unité administrative
CP	Chef de projet
SLA	Service Level Agreement
RSys	Responsable de système
OLPD	Ordonnance relative à la loi sur la protection des données (RS 235.11)

2.14 Définitions

Notion	Définition
Traitement	Toute opération relative à des données personnelles – quels que soient les moyens et procédés utilisés – notamment la collecte, la conservation, l'exploitation, la modification, la communication, l'archivage ou la destruction de données (art. 3, let. e, LPD).
Communication	Le fait de rendre des données personnelles accessibles, par exemple en autorisant leur consultation, en les transmettant ou en les diffusant (art. 3, let. f, LPD).
Données sensibles	Les données personnelles sur les opinions ou activités religieuses, philosophiques, politiques ou syndicales, sur la santé, la sphère intime ou l'appartenance à une race, sur des mesures d'aide sociale, et sur des poursuites ou sanctions pénales et administratives (art. 3, let. c, LPD).
Fichier	Au sens de la loi sur la protection des données, est réputé fichier « tout ensemble de données personnelles dont la structure permet de rechercher les données par personne concernée » (art. 3, let. g, LPD).
Maître du fichier	La personne privée ou l'organe fédéral qui décide du but et du contenu du fichier (art. 3, let. i, LPD).
Données personnelles	Toutes les informations qui se rapportent à une personne identifiée ou identifiable, y compris les personnes morales (art. 3, let. a et b, LPD).
Profil de la personnalité	Un assemblage de données qui permet d'apprécier les caractéristiques essentielles de la personnalité d'une personne physique (art. 3, let. d, LPD).