Règlement relatif au traitement des données d'EGK-Caisse de santé

EGK-Caisse de Santé regroupe la Fondation EGK-Caisse de Santé et ses sociétés anonymes affiliées: EGK Assurances de Base SA (assureur de l'assurance obligatoire des soins selon la LAMal), EGK Assurances Privées SA (assureur des assurances complémentaires selon la LCA) et EGK Services SA.

EGK-Caisse de Santé
Birspark 1, 4242 Laufon
T 061 765 51 11
info@egk.ch, www.egk.ch

Sommaire

Liste des abréviations

Terme	Description
LPGA	Loi fédérale du 6 octobre 2000 sur la partie générale du droit des assurances sociales (RS 830.1)
OFSP	Office fédéral de la santé publique
Cent	Cent Systems AG
Centris	Centris AG
SRD	Service de réception des données
DRG	Diagnosis Related Groups (groupes de cas liés au diagnostic)
LPD	Loi fédérale du 1er septembre 2023 sur la protection des données (RS 235.1)
OLPD	Ordonnance du 1er septembre 2023 sur la protection des données (RS 235.11)
PFPDT	Préposé fédéral à la protection des données et à la transparence
FINMA	Autorité fédérale de surveillance des marchés financiers
IaaS	Infrastructure as a Service
LAMal	Loi fédérale du 18 mars 1994 sur l'assurance-maladie (RS 832.10)
LSAMal	Loi fédérale du 26 septembre 2014 sur la surveillance de l'assurance-maladie sociale (RS 832.12)
MCD	Minimal Clinical Dataset
SaaS	Software as a Service
SFTP	Secure File Transfer Protocol
SHP	Swiss Health Platform
SPS	Swiss Post Solutions SA
SMC	Service du médecin-conseil
LCA	Loi fédérale du 2 avril 1908 sur le contrat d'assurance (RS 221.229.1)

1 Généralités

1.1 Champ d'application

Le présent règlement relatif au traitement des données (ci-après «règlement») d'EGK-Caisse de santé (ci-après «EGK») s'applique à toutes les entités affiliées au groupe EGK. Les données personnelles sont traitées d'une part par EGK Assurances de Base SA dans le domaine de l'assurance-maladie sociale (assurance obligatoire des soins et assurance facultative d'indemnités journalières), et d'autre part par EGK Assurances Privées SA dans le domaine de l'assurance-maladie complémentaire privée. De son côté, EGK Services SA fournit des prestations d'administration et de service pour toutes les entités du groupe EGK.

Le présent document veille à une formulation dite épicène. Quand cela n'est pas possible, un seul genre est utilisé pour une meilleure lisibilité du texte, mais toutes les personnes n'en sont pas moins désignées.

1.2 Base juridique

EGK traite les données personnelles conformément aux dispositions de la LPD. En sa qualité d'organe fédéral et d'assurance-maladie agréée selon la LSAMal, elle est légalement habilitée à traiter des données personnelles dans le domaine de la LAMal. En tant que prestataire d'assurances-maladie complémentaires selon la LCA, elle traite également les données personnelles en tant que personne morale privée sur la base des contrats d'assurance conclus avec la clientèle.

En vertu de l'art. 6 OLPD en relation avec l'art. 84b LAMal, EGK a établi le présent règlement pour le traitement automatisé de données qui contiennent des informations sensibles ou un profilage. EGK traite les données pour accomplir ses tâches d'assurance-maladie sociale et privée. Au sens de l'art. 12 al. 1 et 4 en relation avec l'art. 56 LPD, EGK est tenue, en tant qu'organe fédéral, d'annoncer le traitement de données personnelles au PFPDT, qui publie l'annonce dans un registre accessible au public (https://datareg.edoeb.admin.ch/search).

1.3 Objectif du règlement

Le règlement définit les procédures de traitement des données et de contrôle, ainsi que l'exploitation du traitement électronique des données d'EGK. Il contient des indications sur les domaines et les personnes responsables de la protection des données et de la sécurité des données, sur l'origine des données et la finalité de leur traitement. Il décrit la procédure d'octroi des autorisations d'accès aux différents modules des systèmes d'information électroniques.

1.4 Service responsable

La direction d'EGK est responsable des décisions dans le sens de la finalité et des moyens du traitement des données.

1.5 Externalisation

Le traitement des données personnelles peut être confié à des tiers en vertu de la loi ou d'un accord (externalisation). Les principaux services externalisés font partie des informations sur le plan d'affaires soumises à l'autorisation des autorités de surveillance (OFSP pour l'assurance-maladie sociale selon la LAMal et FINMA pour les assurances-maladie complémentaires selon la LCA).

Les prestataires sont tenus de traiter les données mises à leur disposition exclusivement dans le cadre défini contractuellement, de la même manière dont EGK est censée les traiter conformément aux normes légales applicables, sauf si une obligation de confidentialité légale ou contractuelle l'interdit.

1.6 Obligation de garder le secret en vertu de l'art. 33 LPGA

Tous les membres du personnel d'EGK sont soumis à l'obligation de garder le secret en vertu de l'art. 33 LPGA. En outre, ils signent avec le contrat de travail une déclaration de confidentialité et d'obligation de garder le secret. De même, les dispositions relatives au secret et à la confidentialité du code de conduite d'EGK s'appliquent.

1.7 Service certifié de réception des données

Le SRD d'EGK requis par la loi est géré par la société Centris à Soleure, qui propose cette prestation de services à plusieurs assureurs-maladie. Le domaine de certification du SRD (*scope*) ne s'étend pas seulement à Centris et à son SRD, mais aussi à des domaines partiels d'EGK, de SPS et de Cent (voir aussi chapitre 2 Modèle d'exploitation informatique et interfaces).

2 Modèle d'exploitation informatique et interfaces

2.1 Modèle d'exploitation

Pour l'exercice de ses activités dans le cadre de l'assurance-maladie sociale et de l'assurance-maladie complémentaire privée, EGK a recours, en plus de ses propres services commerciaux informatiques, à ceux de prestataires informatiques triés sur le volet sous la forme d'IaaS et de SaaS. Le système central d'assurance-maladie est constitué de la SHP de Centris.

2.2 Interfaces

EGK reçoit des données de sa clientèle et de ses prestataires. Les factures électroniques sont transmises dans le format approprié par les fournisseurs de prestations directement à Centris ou au SRD qu'elle exploite. Les justificatifs de facture sur papier sont scannés par SPS et transmis pour la saisie des factures (reconnaissance) à Cent, qui fournit ensuite les données dans le format approprié pour leur traitement consécutif chez Centris. Les lettres de correspondance et les formulaires sont importés dans le système central d'assurance-maladie SHP de Centris après avoir été numérisés par SPS.

EGK et ses prestataires utilisent des procédures de cryptage symétriques et asymétriques modernes pour l'échange de données. Des interfaces sécurisées permettent le contact et l'échange électronique de données avec la clientèle, les fournisseurs de prestations, les autorités et les prestataires.

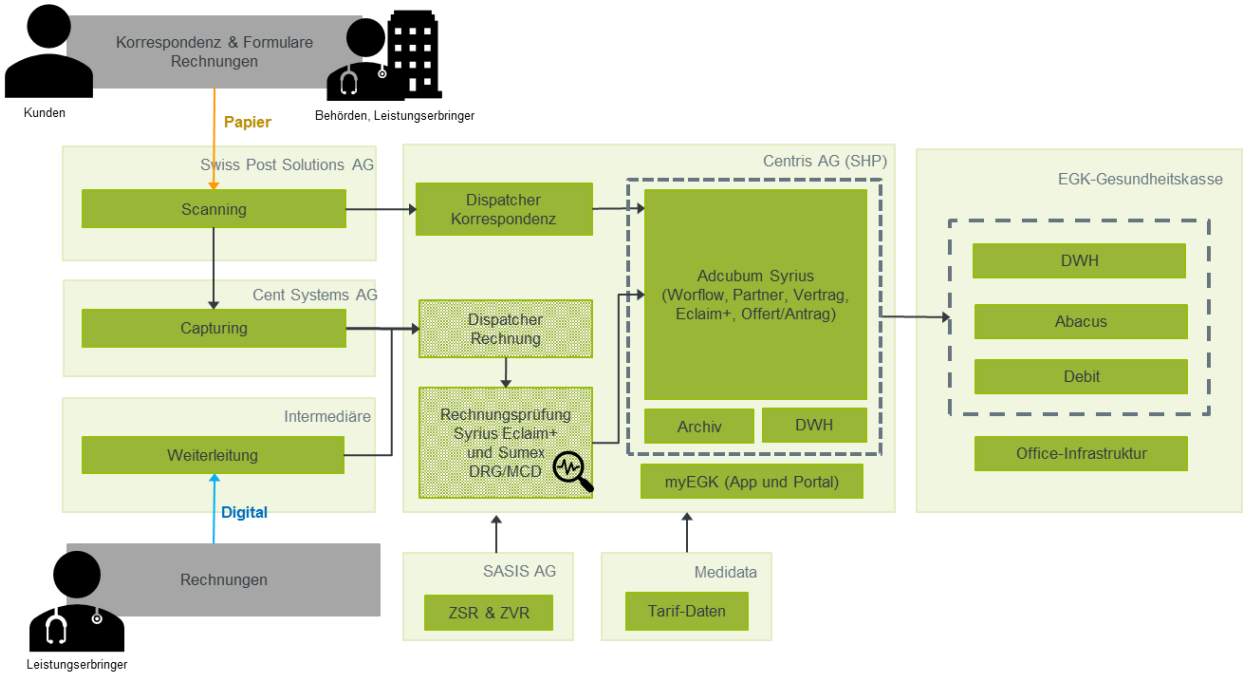

Illustration 1 Aperçu sommaire des interfaces

Von	Nach	Zweck beim Empfänger	Daten
Versicherte Leistungserbringer Behörden	SPS	Digitalisieren von Papierdokumenten (Korrespondenz/Formulare, Rechnungen) und Zuweisen des Dokumenttyps	Dokumente in Papierform (Belege, Formulare)
SPS	CENT	Datenweiterleitung der Belege zur Erkennung und Erfassung (Capturing) des Dokumenteninhalts	TIFF mit Metainformationen
SPS	Centris	Datenweiterleitung der Korrespondenz/Formulare für die Verarbeitung über das Workflowsystem	PDF mit Metainformationen
CENT	Centris	Datenweiterleitung zur Rechnungsprüfung	Elektronische Rechnungen nach Standard Forum Datenaustausch (XML 4.x)
Intermediäre	Centris	Datenweiterleitung zur Rechnungsprüfung	Elektronische Rechnungen nach Standard Forum Datenaustausch (XML 4.x)
Centris	EGK	DWH: Reports und Datenanalysen für interne geschäftliche Zecke und Behörden	Personenstammdaten, Vertragsdaten, Leistungsdaten
Centris	EGK	Debit: Bearbeitung von Inkassofällen	Betreibungsinformationen
Centris	Ämter	Austausch an Betreibungsämter (eSchKG) für rechtliches Inkasso und DA 64 mit Kantonen (Leistungsaufschub, Quartalsabrechnungen Verlustscheine)	Partnerstammdaten (Schuldnerangaben) und offene Forderungen
SASIS AG	Centris	Zahlstellenregister und zentrales Vertragsregister der Leistungserbringer	Adressstammdaten und Tarifpreise der Leistungserbringer
Medidata	Centris	Tarifdaten	Tarifdaten des schweizerischen Gesundheitssystems (Taxpunkte)

Illustration 2: Description des interfaces

2.3 Responsables de processus

Les responsables de processus et les utilisateurs finaux veillent au respect des dispositions légales et contractuelles, des instructions et des règles internes relatives au traitement des données, en particulier dans les domaines de la sécurité et de la protection des données.

Ils sont chargés de s'assurer que les données d'application sont uniquement mises à disposition en conformité avec les bases juridiques ou les restrictions étendues sur la base du présent règlement, de la politique de sécurité de l'information d'EGK et des instructions internes.

EGK définit également les responsabilités à chaque fois que des données à caractère personnel sont traitées (voir chapitre 4.5 Liste des activités de traitement).

3 Personnes participant au traitement des données

3.1 Types d'utilisateurs et droits d'accès correspondants

- Membres du personnel d'EGK, dans la mesure où ils en ont besoin pour l'exécution de leur mandat
- Membres du personnel d'entreprises de service externes, dans la mesure où ils en ont besoin pour l'exécution de leur mandat et conformément aux prescriptions contractuelles et légales (voir aussi chapitre 1.5 Externalisation)

Disposent d'autorisations complémentaires d'accès au MCD:

- spécialistes DRG / du codage (2 personnes)

Autorisations d'accès supplémentaires aux documents du SMC:

- collaborateurs du SMC

3.2 Gestion des utilisateurs

Les droits d'utilisateurs sont conçus et structurés sur la base des rôles. Le service spécialisé compétent est chargé de la définition des différents rôles d'utilisateurs. La personne chargée de la protection des données surveille les exigences légales en matière de protection des données et le principe de la séparation des pouvoirs.

La gestion des droits d'utilisateur est basée sur un processus standard défini (entrée, mutation, sortie). Les membres du personnel reçoivent uniquement l'autorisation d'accéder aux données nécessaires à leur travail (principe «need to know»). En cas de mutations (p. ex. changement de département), les autorisations sont adaptées en conséquence. L'accès aux données est bloqué aux membres du personnel quittant EGK, au plus tard à partir du dernier jour de travail.

Dans le cadre de la formation de base d'EGK et au sein de leur unité, les membres du personnel suivent une formation sur la protection des données en fonction des tâches à assumer. De plus, le thème de la protection des données fait partie intégrante des formations de *compliance* annuelles, et il existe un programme destiné à sensibiliser régulièrement les membres du personnel. Par ailleurs, les cours sur la protection des données de l'association de branche sont ouverts aux membres du personnel. Ces cours sont obligatoires pour les spécialistes DRG ainsi que les membres du personnel du SMC.

4 Procédures de traitement des données

4.1 Finalité du traitement des données

Dans le domaine de l'assurance obligatoire des soins et de l'assurance facultative d'indemnités journalières selon la LAMal, EGK traite les données conformément aux droits et obligations légaux relatifs à l'exercice de l'activité d'assurance. Dans le domaine des assurances complémentaires des soins selon la LCA, le traitement des données a lieu aux fins de l'exécution des droits et obligations contractuels relatifs à l'exercice de l'activité d'assurance. Le traitement des données documente notamment les rapports d'assurance dans le cadre de la conclusion du contrat, du traitement des paiements ainsi que du contrôle et du règlement des droits aux prestations des personnes assurées.

4.2 Origine des données et catégories de données

Les données proviennent d'une part des personnes assurées et d'autre part de personnes physiques et morales telles que les fournisseurs de prestations, les assurances et les autorités qui ont été autorisées par la loi ou avec le consentement des personnes assurées à transmettre des données.

Les informations ci-après des données personnelles traitées sont catégorisées dans les applications respectives conformément à l'art. 12, al. 2, let. c, LPD et protégées contre toute consultation non autorisée:

- nom, prénom, adresse, numéros de téléphone, (e-mail);
- date de naissance;
- numéro d'assurance;
- numéro d'assurance sociale;
- langue et nationalité;
- situation familiale et représentation légale;
- informations relatives à la santé;
- mesures d'aide sociale;
- données sur les prestations;
- données sur les primes;
- coordonnées de paiement;
- données de rappel et d'encaissement.

4.3 Communication de données

Dans le domaine de l'assurance de base, les données sont communiquées dans le cadre des dispositions de l'art. 84a LAMal. Dans le domaine des assurances complémentaires, les données sont communiquées sur la base du contrat d'assurance conclu. Dans tous les autres cas, la communication des données à des tiers se fait sur la base du consentement écrit de la personne concernée.

4.4 Durée de conservation et effacement des données

La durée minimale de conservation dépend de l'obligation légale spécifique de conservation selon les dispositions déterminantes du droit suisse. Les données sont protégées contre toute modification et tout accès non autorisé et effacées du système d'information d'EGK quand l'obligation de conservation prend fin.

4.5 Liste des activités de traitement

EGK tient une liste des activités de traitement de l'ensemble des données à caractère personnel, qui fournit notamment des informations sur les responsabilités, la finalité du traitement et la durée de conservation des données personnelles correspondantes.

4.6 Procédure d'anonymisation des données

Dans la mesure du possible, les tests doivent être effectués à l'aide de fichiers de données anonymes. En outre, lorsque la loi l'exige, les données utilisées à des fins statistiques sont toujours anonymisées.

5 Sécurité des données

EGK protège ses systèmes par des autorisations d'accès au moyen du nom d'utilisateur, d'un mot de passe et d'autres facteurs supplémentaires le cas échéant. En outre, l'accès aux applications permettant de consulter des données personnelles est limité dans le temps. Si l'application n'est pas utilisée pendant un certain temps, une nouvelle connexion à l'aide du mot de passe est nécessaire.

5.1 Mesures techniques et organisationnelles

En vertu de l'art. 3 OLPD, EGK protège ses systèmes contre la destruction non autorisée ou accidentelle, la perte accidentelle, les erreurs techniques, la falsification, le vol ou l'utilisation illicite et le traitement non autorisé. Pour cela, elle a pris les mesures générales suivantes:

- Les données se trouvent dans des centres de calcul sécurisés par des moyens techniques et des mesures organisationnelles ultramodernes. Les locaux spéciaux abritant des installations techniques informatiques bénéficient d'une sécurité supplémentaire.
- Lors d'échanges d'e-mails individuels, la procédure de cryptage doit être utilisée en cas de transmission de données personnelles sensibles (notamment données de santé).
- Les destinataires auxquels des données personnelles sont communiquées au moyen de dispositifs de transfert de données sont identifiés par les interfaces. Les transmissions régulières de données personnelles ont toujours lieu de manière standardisée par un canal crypté (p. ex. SFTP).
- Seuls les terminaux propres à EGK peuvent être rattachés au réseau interne. Les interfaces pour un éventuel échange de données sont verrouillées et réservées à un cercle restreint de personnes.
- Les exportations de données vers d'autres supports de stockage (p. ex. clé USB) sont rendues techniquement impossibles.
- Les mémoires locales sur les terminaux mobiles sont cryptées par un procédé cryptographique efficace et protégées par un mot de passe.

Les mesures techniques et organisationnelles sont brièvement expliquées ci-après.

5.1.1 Contrôle d'accès numérique

Seules les personnes autorisées ont accès à la SHP, à ses systèmes périphériques et aux systèmes propres à EGK (principe «need to know»). L'accès aux systèmes d'information propres à EGK est protégé par un nom d'utilisateur combiné à un mot de passe individuel valable pour une durée limitée (conformément à la directive sur les mots de passe d'EGK). La directive sur les mots de passe est imposée par des prescriptions techniques correspondantes. Certains systèmes font l'objet d'une protection supplémentaire par l'utilisation d'un autre mot de passe.

5.1.2 Contrôle d'accès physique

L'accès aux locaux d'EGK est sécurisé par un système de badge contre l'entrée de personnes non autorisées. Des zones de conseil spécialement aménagées et des mesures spatiales empêchent la consultation ou l'accès de tiers non autorisés à des locaux ou des zones dans lesquels des données personnelles sont traitées.

Les tiers n'ont accès aux postes de travail que moyennant l'accord d'EGK et avec un badge visiteur ou en

compagnie de membres du personnel. Les visiteurs doivent toujours s'inscrire à la réception, où leur est remis le badge visiteur, qui doit être porté de façon bien visible.

En outre, l'accès aux locaux dans lesquels des données sensibles sont disponibles ou traitées (SMC, locaux techniques, etc.) est limité au cercle nécessaire des membres du personnel.

5.1.3 Contrôle des utilisateurs

L'octroi des droits d'utilisateur ainsi que les éventuelles modifications des autorisations existantes interviennent selon un processus d'autorisation clairement défini. Les autorisations existantes sont régulièrement vérifiées et adaptées si nécessaire. En cas de mutations (p. ex. changement de département), les autorisations sont adaptées en conséquence. En cas de départ de l'entreprise, l'accès aux données est bloqué au plus tard à partir du dernier jour de travail.

5.1.4 Contrôle des supports de données

Les données sont exclusivement traitées à distance. En outre, l'octroi des autorisations d'accès garantit que les membres du personnel ne peuvent accéder qu'aux données nécessaires à l'accomplissement de leur travail (principe «need to know»), empêchant ainsi toute personne non autorisée de lire, copier, modifier ou effacer des données.

5.1.5 Contrôle de la mémoire

Grâce à des mesures de sécurité, seules les personnes autorisées peuvent consulter, traiter ou stocker des données dans le système d'information d'EGK. L'entrée non autorisée dans la mémoire ainsi que la consultation, la modification ou l'effacement non autorisés des données personnelles enregistrées sont ainsi rendus impossibles.

5.1.6 Contrôle du transport

Si des données sont échangées ou transmises à des tiers, le transfert a toujours lieu par des canaux cryptés (voir également chapitre 2).

5.1.7 Restauration

En collaboration avec ses partenaires d'externalisation dans le domaine des prestations et services informatiques, EGK garantit une reprise aussi rapide que possible des processus commerciaux tout au long de la chaîne de processus grâce aux mesures BCM définies.

5.1.8 Disponibilité, fiabilité, intégrité des données

L'assurance est donnée que la disponibilité et l'intégrité des données des personnes assurées, des membres du personnel et des partenaires sont garanties en tout temps et qu'elles sont traitées de manière confidentielle et conforme aux règles de protection des données.

5.1.9 Sécurité du système

EGK s'assure, par des mesures appropriées, que les systèmes d'exploitation et les logiciels d'application sont toujours à la pointe de la sécurité et que les lacunes critiques connues sont comblées.

5.1.10 Contrôle des entrées (journalisation)

Un contrôle de saisie et de modification de toutes les mutations est effectué. Il est ainsi possible de vérifier a posteriori quelles données personnelles ont été saisies, à quel moment et par quelle personne.

5.1.11 Contrôle de la notification

EGK veille à ce que les destinataires auxquels des données personnelles sont communiquées au moyen de dispositifs de transfert de données puissent être identifiés via les interfaces.

5.1.12 Détection et élimination

EGK veille à ce que les violations de la sécurité des données soient rapidement détectées au moyen de mesures appropriées et à ce que des mesures soient prises pour en atténuer ou éliminer les conséquences.

6 Droits des personnes concernées

6.1 Droit d'accès

Toute personne peut se renseigner auprès d'EGK afin de savoir si des données la concernant font l'objet d'un traitement. Le droit d'accès est régi par les art. 25 et 26 LPD ainsi que par les art. 16 à 19 OLPD. La demande de renseignements doit être adressée à la personne chargée de la protection des données (datenschutz@egk.ch) en joignant une copie d'une pièce d'identité officielle.

6.2 Portabilité des données

Toute personne peut exiger d'EGK qu'elle lui communique les données personnelles qu'elle lui a communiquées dans un format électronique courant et, si cela n'exige pas d'efforts disproportionnés, le transfert de ses données personnelles à un autre responsable, si les conditions de l'art. 28, al. 1, let. a et b LPD sont remplies.

6.3 Opposition à la communication

La personne concernée qui rend vraisemblable un intérêt digne de protection peut s'opposer à ce que l'organe fédéral responsable communique des données personnelles déterminées. Ce droit est régi par l'art. 37 LPD. S'il existe une obligation légale de communication ou si l'accomplissement des tâches de l'organe fédéral responsable risque d'être compromis, la demande est rejetée.

6.4 Droit de rectification et d'effacement

Le droit de rectification et d'effacement des personnes concernées est régi par les art. 32 et 41 LPD, dans le respect des obligations de conservation légales et/ou contractuelles. Une demande en ce sens est adressée à EGK à l'attention de la personne chargée de la protection des données (datenschutz@egk.ch).

7 Dispositions finales

7.1 Garantie de la protection des données par les assureurs

Le présent règlement a été établi conformément à l'art. 84b LAMal et sert à informer les personnes concernées de leurs droits ainsi qu'à documenter les mesures techniques et organisationnelles visant à garantir la sécurité et la protection des données. Il est publié sur le site Internet d'EGK.

7.2 Documents complémentaires

Pour des raisons de sécurité des systèmes, des processus et des données, de respect de la confidentialité des personnes assurées et de protection des secrets d'affaires d'EGK et de ses partenaires commerciaux, les documents complémentaires mentionnés dans le présent règlement ne sont pas rendus publics.

7.3 Compétence/Vérification

Ce règlement est régulièrement mis à jour par EGK conformément aux art. 5 et 6 OLPD. En collaboration avec les services spécialisés compétents, la personne chargée de la protection des données vérifie au moins une fois par an qu'il est à jour et le fait approuver par la direction. Si nécessaire, il peut être adapté à tout moment.

7.4 Entrée en vigueur

Le présent règlement entre en vigueur le 1er septembre 2023 et remplace la version précédente.