Politique de sécurité de l'information 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
Brislachstrasse 2, 4242 Laufon
T 061 765 51 11
info@egk.ch, www.egk.ch

Distribution: - Direction d'EGK-Caisse de Santé
- Tous les collaborateurs d'EGK-Caisse de Santé (intranet)

Publication: http://www.egk.ch/egk/

Informations importantes relatives au document	
Auteur en charge:	Kilian Schmidlin
Nom du fichier:	Politique de sécurité de l'information d'EGK-Caisse de Santé
Numéro de version:	1.3
Numéro du document:	1.3.02-f
Nombre de pages:	7
Niveau de confidentialité:	V1 - public
Élaboration commencée le:	25.09.2014
Validé le:	20 octobre 2014
Dernière adaptation le:	27 septembre 2018
Statut de traitement:	validé
Dernière validation le:	1er octobre 2018
Validé par:	la direction

Documents complémentaires / autres documents applicables			
Titre du document	*Version*	*Date*	*Auteur responsable*
Règlement sur le traitement relatif à la collecte de données	3.0	22.10.2018	Kilian Schmidlin
Déclaration sur la protection des données pour les services en ligne	1.0	13.06.2018	Stefanie Omlin
Règlement relatif aux moyens informatiques	1.0	26.10.2017	Andrea Grolimund
Concept BCM	2.7	31.08.2018	Patrick Tanner Alice Grolimund Kilian Schmidlin
Concept de sauvegarde des données	1.2	31.10.2016	Patrick Tanner
Directive relative à la classification des données / informations / documents	1.0	01.10.2018	Kilian Schmidlin

I. Sommaire

I. Sommaire 1
II. Liste des abréviations 2
1 Champ d'application 2
2 But 2
3 Objectifs de sécurité d'EGK 2
4 Stratégie d'approvisionnement informatique 3
5 Principes 3
5.1 Prescriptions, lois et contrats 3
5.2 Objectifs de sécurité informatique 3
5.2.1 Confidentialité 4
5.2.2 Disponibilité 4
5.2.3 Intégrité 4
6 Responsabilité 4
7 Processus de traitement des dérogations et des exceptions. 4
8 Vérification 5
9 Suivi des modifications 5

II. Liste des abréviations

BCM	Business Continuity Management (En français: gestion de la continuité dans l'entreprise)
CENT	Cent Systems AG
SRD	Service de réception des données
DRG	Diagnosis Related Groups (En français: groupes de cas liés au diagnostic pour les factures d'hôpital stationnaires)
LPD	Loi sur la protection des données
PFPDT	Préposé fédéral à la protection des données et à la transparence
FINMA	Autorité fédérale de surveillance des marchés financiers
TIC	Information and communications technology (En français: technologie de l'information et de la communication)
LAMal	Loi sur l'assurance-maladie
MCD	Minimal Clinical Dataset (En français: jeu de données médicales)
ROC	Optical character recognition (En français: reconnaissance optique de caractères)
SHP	Swiss Health Platform (application centrale d'EGK/de Centris AG)
SPS	Swiss Post Solutions, filiale de Swiss Post
LCA	Loi sur le contrat d'assurance

1 Champ d'application

La raison sociale de l'entreprise, EGK-Caisse de Santé, ci-après EGK, regroupe la fondation EGK-Caisse de santé et ses sociétés anonymes lui étant 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. La politique de sécurité de l'information d'EGK s'applique à toutes les sociétés du Groupe EGK.

2 But

Conformément à la vision d'EGK-Caisse de Santé, nous protégeons et respectons la vie privée de nos clients. En d'autres termes, nous gérons avec soin les données qui ont été mises à notre disposition et que nous traitons. Le code de conduite et plusieurs règlements le prévoient également. Ces principes fixent le cadre de la politique de sécurité de l'information d'EGK.

Les informations et données, notamment les données personnelles et médicales des assurés, revêtent une importance centrale pour l'exécution de notre mandat légal selon la LAMal dans l'assurance obligatoire des soins (assurance de base) ainsi que pour le traitement conforme au contrat des assurances complémentaires selon la LCA. Nos mesures de protection des données et de sécurité servent à empêcher autant que possible les événements dommageables, à réduire leur fréquence et leurs conséquences ainsi qu'à les maintenir dans un cadre supportable et proportionné.

3 Objectifs de sécurité d'EGK

- Maintien des principaux centraux de l'entreprise.
- Niveau de sécurité élevé, stabilité, continuité et qualité du traitement des données et informations ainsi que de la fourniture de prestations de services compte tenu des prescriptions légales, du principe de la proportionnalité et des aspects liés à l'acceptabilité économique.

- Prévention de dommages de réputation ou de dommages financiers pour EGK du fait de la perte de données ou d'informations ou de la prise de connaissance de données et d'informations par des tiers non autorisés.
- Grande sensibilisation des collaborateurs de tous les échelons et de tous les départements sur les questions de sécurité et de protection des données.

4 Stratégie d'approvisionnement informatique

EGK mise sur une stratégie d'outsourcing partielle des prestations informatiques en externalisant et en déléguant de manière ciblée les prestations d'ingénierie et d'exploitation. L'application centrale d'assurance est ainsi externalisée auprès de Centris AG à Soleure. Cette société est un prestataire professionnel certifié du secteur, qui exploite la «Swiss Health Platform» SHP pour plusieurs assureurs-maladie. Centris AG exerce également la fonction de service certifié de réception des données (SRD) d'EGK pour le processus électronique dans le domaine des factures de type DRG. À cet effet, elle est inscrite et reconnue en tant que telle auprès du Préposé fédéral à la protection des données et à la transparence (PFPDT). Font notamment partie de l'environnement de la SHP les systèmes Syrius ASE, CBPM, SUMEX II, DWH, OD, le système d'archivage FileNet, Massprinting et la Digital Insurance Platform (DIP).

Par ailleurs, EGK recourt aux prestations informatiques d'Econis AG pour l'infrastructure et le fonctionnement de base du centre de données dans le cadre d'une infogérance. Par infogérance, on entend le fonctionnement du matériel informatique dans le domaine du stockage sur serveur et de l'accès à distance.

Les TIC d'EGK conservent la souveraineté à partir du niveau des systèmes d'exploitation de l'infrastructure de la base de données opérationnelle (serveur HW et OS) pour les systèmes périphériques d'EGK.

L'infrastructure du réseau et les prestations de téléphonie sont fournies par Swisscom.

Parmi les autres partenaires externes importants d'EGK pour le traitement des données figurent Swiss Post Solutions (SPS) en tant que prestataire de numérisation et Cent Systems SA (Cent) pour le Capturingservice.

5 Principes

5.1 Prescriptions, lois et contrats

- Les dispositions légales, contractuelles et internes doivent être systématiquement respectées lors du traitement de données et d'informations.
- Dans le cas de données et d'informations confidentielles d'assurés, les dispositions spéciales de la loi fédérale sur la protection des données (LPD) et de la loi fédérale sur l'assurance-maladie (LAMal) doivent être observées.
- En vertu de l'art. 84b LAMal, un règlement sur le traitement des données doit être établi et rendu public.
- La continuité de l'activité opérationnelle doit également être garantie en cas d'évènements et de situations extraordinaires, et les standards minimaux relatifs aux compagnies d'assurance reconnus par la FINMA doivent être respectés (BCM).
- La conservation de données, d'informations et de documents est soumise aux prescriptions légales; en cas de doute, un délai de conservation d'au moins 10 ans est applicable.

5.2 Objectifs de sécurité informatique

- Il convient d'assurer que la disponibilité, l'intégrité et le traitement confidentiel des données et informations d'EGK et de ses assurés, collaborateurs et partenaires sont garantis en tout temps. À cet égard, les principes suivants s'appliquent:

5.2.1 Confidentialité

- Si des données et informations sont transmises à des tiers, la manière dont ces informations peuvent être utilisées, traitées et exploitées doit être convenue contractuellement. La transmission de données s'effectue de manière anonyme ou via des supports de données et canaux cryptés.

- Lors de l'échange individuel d'e-mails, la procédure de cryptage doit être utilisée en cas de transmission de données à caractère personnel. Le système de messagerie d'EGK offre cette possibilité.

- Les collaborateurs bénéficient d'une formation initiale et continue sur la protection des données et la sécurité de l'information. Il convient de garantir qu'ils connaissent et respectent les règlements de traitement applicables à leur domaine.

- Les données et informations doivent être classifiées à des fins de protection. Les niveaux de classification sont indépendants de l'application sur laquelle les données et informations sont mises à disposition.

5.2.2 Disponibilité

- Un concept de sauvegarde des données doit être établi et déterminer les conditions-cadres des mesures organisationnelles et techniques de sécurité des données.

- Les modifications des applications doivent être apportées selon un processus de Change Management défini.

- Les collectes de données personnelles doivent être gérées dans un répertoire de traitement des données indiquant l'endroit où les données sont enregistrées et la façon dont les délais de suppression sont définis.

5.2.3 Intégrité

- En vue de la protection des informations, les clés cryptographiques doivent être munies d'une date de fin prévisible ne pouvant être éloignée de plus de trois ans.

- Un concept d'autorisation basé sur les fonctions doit garantir que les collaborateurs n'ont accès qu'aux données et informations dont ils ont besoin dans le cadre de leur activité.

- Des mécanismes de protection doivent garantir que seuls les collaborateurs autorisés peuvent installer eux-mêmes des fichiers exécutables.

6 Responsabilité

La responsabilité de la sécurité des données et informations ainsi que de la disponibilité et de l'intégrité des données incombe au responsable TIC d'EGK.

Les responsables de département ainsi que les cadres dirigeants des différents départements sont responsables de la mise en œuvre au sein de leur domaine de compétence.

Les collaborateurs sont appelés à signaler tout problème de protection des données ou de sécurité constaté ou présumé à la direction du département ou au responsable de la protection des données de l'entreprise.

7 Processus de traitement des dérogations et des exceptions.

Les exceptions et les dérogations qui sont en contradiction avec la politique de sécurité de l'information doivent être transmises à la direction à des fins de vérification et d'approbation sur la base d'une demande correspondante.

8 Vérification

Ce document relatif à la politique de sécurité de l'information est entré en vigueur le 20.10.2014. Il est mis à jour chaque année et les adaptations nécessaires sont alors examinées. Les changements entrent en vigueur après leur validation par la direction.

9 Suivi des modifications

Suivi des modifications				
Numéro de version	*Statut de traitement*	*Date*	*Personne chargée du traitement*	*Modification/remarque*
0.1	Version initiale	25.09.2014	K. Schmidlin	
1.0	Validé le	20.10.2014	K. Schmidlin	
1.1	Validé le	03.10.2016	K. Schmidlin	- Adaptations au nouvel environnement système SHP
1.2	Validé le	25.09.2017	K. Schmidlin	- Intégration BCM - Diverses petites adaptations.
1.3	Validé le	01.10.2018	P. Tanner	- Adaptations au chapitre 4 - Nouveaux chapitres 5.1, 5.2 et 7 - Petites adaptations rédactionnelles