Règlement de traitement portant sur le fichier de la fondation Caisse d'indemnités journalières pour artistes selon la LAMal

1. Dispositions générales

1.1 Base légale

La fondation de la Caisse d'indemnités journalières pour artistes a rédigé le présent règlement de traitement pour le fichier automatisé, s'appuyant sur l'art. 21 de l'Ordonnance relative à la loi fédérale sur la protection des données (OLPD), en liaison avec l'art. 84 de la loi fédérale sur l'assurance-maladie (LAMal).

1.2 Objectif du règlement de traitement

Ce règlement de traitement a trait aux procédés de traitement de données et de contrôle et à l'exploitation du traitement de données électronique. Il contient des indications relatives à l'organe en charge de la protection et de la sécurité des données, à l'origine des données et aux fins auxquelles elles sont transmises ainsi que la description du procédé de distribution des autorisations d'accès aux produits des systèmes d'information électroniques.

1.3 Objectif du traitement de données

L'objectif d'un fichier, tel qu'il est énoncé par l'art. 84 de la loi fédérale sur l'assurance-maladie (LAMal) est le suivant:

> *«Les organes chargés d'appliquer la présente loi ou d'en contrôler ou surveiller l'exécution sont habilités à traiter et à faire traiter les données personnelles, y compris les données sensibles et les profils de la personnalité, qui leur sont nécessaires pour accomplir les tâches que leur assigne cette loi, notamment pour:*
>
> *a) veiller au respect de l'obligation de s'assurer;*
>
> *c) établir le droit aux prestations, les calculer, les allouer et les coordonner avec celles d'autres assurances sociales;*
>
> *e) faire valoir une prétention récursoire contre le tiers responsable;*
>
> *f) surveiller l'exécution de la présente loi;*
>
> *g) établir des statistiques;*

h) attribuer ou vérifier le numéro d'assuré AVS.»

La raison d'être de la fondation consiste à exploiter une caisse d'indemnités journalières au profit d'artistes, conformément aux dispositions de la loi fédérale sur l'assurance maladie (LAMal). La fondation ne poursuit pas de but lucratif, d'éventuels bénéfices sont réinvestis; la fortune est uniquement destinée à l'assurance d'indemnités journalières ou à l'assurance accidents le cas échéant, dans la mesure prévue par les règlements.

Ainsi, le fichier de la fondation est réservé au même objectif.

1.4 Responsable

La fondation de la Caisse d'indemnités journalières pour les artistes est une Caisse d'indemnités journalières «pure», en vertu de l'art. 1a, al. 1, en liaison avec l'art. 67 f. LAMal. La fondation, ou ses organes, sont responsables du traitement et de la gestion de données (en conformité avec la protection des données et la sécurité système). La fondation est propriétaire ou «owner» du fichier et des systèmes informatiques. La fondation s'assure du respect des prescriptions la concernant par les mesures décrites.

La responsabilité de la protection et de la sécurité des données incombe à la fondation, ou à ses organes.

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

Tous les collaborateurs de la fondation ou les tiers impliqués sont soumis à l'obligation de garder le secret en vertu de l'art. 33 LPGA.

En cas de violation de l'obligation de garder le secret, les dispositions pénales de l'art. 92 LAMal relevant du droit spécial s'appliquent. Les collaborateurs signent - en plus du contrat de travail - l'obligation de garder le secret et de respecter la confidentialité.

1.6 Externalisation de prestations

La gestion, de même que la comptabilité de la fondation, sont assurées par Swiss Life SA. Les mesures définies dans ce règlement s'appliquent par analogie à cette dernière.

Le contrat d'externalisation conclu avec Swiss Life mentionne clairement que Swiss Life est tenue de respecter les mêmes prescriptions que la fondation lorsqu'elle traite des données. Ceci garantit la conformité à l'objectif poursuivi. Le respect des règles émises par la fondation se voit ainsi contractuellement assuré.

Le respect des conditions imposées par la protection des données est régulièrement vérifié par la fondation au moyen de contrôles effectués par le biais de ses organes.

La transmission des données entre la fondation et Swiss Life est soumise à une réglementation.

2. Fichier

2.1 Structure du fichier

Le fichier de la fondation se compose des systèmes et contenus suivants:

- KUBIK, système de saisie de la fondation Caisse d'indemnités journalières. Seule la fondation Caisse d'indemnités journalières emploie ce système. Les données d'assurés suivantes sont entrées dans le système:

- nom, adresse, numéro d'assuré, date de naissance, sexe, date d'entrée, âge de la retraite (h/f), section de l'association professionnelle regroupant des artistes, lieu de paiement ainsi que la mention d'une éventuelle réserve d'admission;

- sinistre, date de saisie, gravité et durée de la maladie, droit aux prestations et date de paiement;

- informations de comptabilitsation destinées au système de comptabilisation SAP (informations relatives au comptage).

2.2 Interfaces

Seuls les preneurs d'assurance, ou directement leur médecin de confiance transmettent les données personnelles à la fondation. La fondation Caisse d'indemnités journalières vérifie auprès des associations professionnelles regroupant des artistes si le preneur d'assurance est membre de l'Association professionnelle des arts visuels «Visarte», de la Société suisse des femmes artistes en arts visuels «SSFA» ou de l'Association Suisse des PME «SKV».

La protection et la sécurité des données sont assurées par des méthodes d'identification et d'authentification strictes et des technologies de cryptage et de transmission extrêmement pointues.

3. Parties concernées

3.1 Fondation

La fondation de la Caisse d'indemnités journalières pour artistes est propriétaire du fichier et des données.

3.2 Swiss Life

La gestion de même que la comptabilité de la fondation sont assurées par Swiss Life SA. De ce fait, Swiss Life traite les données de la fondation conformément à leur assignation et de manière confidentielle.

3.3 Autres parties concernées

Pas d'autres personnes impliquées.

3.4 «Owner» de l'application

Les propriétaires de l'information définis, conjointement avec les propriétaires d'application et l'IT - sont en charge de la collecte des données pour la fondation et veillent au respect des dispositions et des instructions relatives à la protection et à la sécurité des données.

4. Utilisateurs et accès aux données

4.1 Utilisateurs

L'accès au fichier et aux données de la fondation est réservé aux seules personnes nommément désignées qui nécessitent ces données pour leur travail quotidien (pour le versement ou la vérification des indemnités journalières).

Pour les administrateurs système ou responsables d'application, l'accès à ces données est restreint à l'usage prévu.

Les collaborateurs appartenant à des prestataires de services tiers ne sont pas autorisés d'accès.

4.2 Gestion des utilisateurs

Des processus et procédures de gestion des utilisateurs documentés, des autorisations et rôles ainsi que les autorisations d'accès spécifiques afférentes sont disponibles pour tous les produits, applications et fichiers. Le responsable des profils d'autorisation compétent (RPA) est en charge de la procédure d'autorisation, en concertation avec les responsables de la fondation. Les demandes d'autorisation sont soumises aux personnes susmentionnées pour vérification, la mise en œuvre incombe ensuite au Service Help Desk.

La procédure d'autorisation d'accès est ainsi gérée par les responsables de la fondation, les personnes autorisées d'accès ne le sont que dans la mesure requise par l'exécution de leurs tâches quotidiennes. Les autorisations sont automatiquement retirées en cas de départ ou de changement d'emploi.

4.3 Formation des utilisateurs

Une formation sur la protection et la sécurité des données est régulièrement prodiguée aux utilisateurs. Cela concerne également le domaine spécifique du traitement des données de la fondation.

5. Traitement des données / catégories de données

5.1 Provenance des données

Les données proviennent en premier lieu des preneurs d'assurance de la Caisse d'indemnités journalières ainsi que de leurs représentants.

5.2 Catégories de données

Les différentes catégories de données de la fondation figurent dans l'annexe 1.

5.3 Classification des données

Les données sont classées confidentielles. Toutes les mesures sont adaptées au niveau de protection élevé. Les règles de traitement sont définies par une instruction et les collaborateurs bénéficient régulièrement d'une formation y afférente.

5.4 Transmission des données

En ce qui concerne la communication de données, l'art. 84a de la LAMal stipule que:

«Dans la mesure où aucun intérêt privé prépondérant ne s'y oppose, les organes chargés d'appliquer la présente loi et d'en contrôler ou surveiller l'application peuvent communiquer des données, en dérogation à l'art. 33 LPGA:

a) à d'autres organes chargés d'appliquer la présente loi ou d'en contrôler ou surveiller l'exécution, lorsqu'elles sont nécessaires à l'accomplissement des tâches que leur assigne la présente loi;

aux organes d'une autre assurance sociale, lorsque, en dérogation à l'art. 32, al. 2, LPGA, l'obligation de les communiquer résulte d'une loi fédérale;

bbis.) aux organes d'une autre assurance sociale, en vue d'attribuer ou de vérifier le numéro d'assuré AVS;

c) aux autorités compétentes en matière d'impôt à la source, conformément aux art. 88 et 100 de la loi fédérale du 14 décembre 1990 sur l'impôt fédéral direct5 et aux dispositions cantonales correspondantes;

d.) aux organes de la statistique fédérale, conformément à la loi du 9 octobre 1992 sur la statistique fédérale6;

e) aux organismes chargés d'établir des statistiques servant à l'exécution de la présente loi, lorsque les données sont nécessaires à l'accomplissement de cette tâche et que l'anonymat des assurés est garanti;

f) aux autorités cantonales compétentes, s'agissant des données visées à l'art. 22a qui sont nécessaires à la planification des hôpitaux et des établissements médico-sociaux ainsi qu'à l'examen des tarifs;

g) aux autorités d'instruction pénale, lorsqu'il s'agit de dénoncer ou de prévenir un crime;

...

5 Dans les autres cas, des données peuvent être communiquées à des tiers, en dérogation à l'art. 33 LPGA:

a) s'agissant de données non personnelles, lorsqu'un intérêt prépondérant le justifie;

b) s'agissant de données personnelles, lorsque la personne concernée y a, en l'espèce, consenti par écrit ou, s'il n'est pas possible d'obtenir son consentement, lorsque les circonstances permettent de présumer qu'il en va de l'intérêt de l'assuré.»

Les données sont communiquées aux fins suivantes:

- l'évaluation de droits aux prestations
- la gestion de la relation contractuelle
- la comptabilité
- la coordination avec d'autres assurances sociales en conformité avec l'examen des requêtes

Les destinataires de données sont listés ci-dessous:

- les personnes assurées et leurs mandataires

- les autorités (Office de AI par exemple)
- Swiss Life
- les médecins de confiance

Les autres points relatifs à la communication des données sont définis par la LAMal.

6. Durée de conservation et suppression des données

Tant la fondation que Swiss Life remplissent les exigeances légales en matière d'archivage. La durée d'archivage après conclusion est également déterminée par les prescriptions légales. Les données sont ensuite effacées et détruites.

7. Mesures techniques et organisationnelles

7.1 Contrôle de l'accès

La sécurité de l'accès suppose que: l'entrée de tous les locaux appartenant à la fondation ou à des tiers impliqués dans lesquels des données personnelles sont traitées soit protégée - manuellement ou électroniquement - de l'intrusion de personnes non autorisées (le bureau principal étant fermé en dehors des heures de service); l'entrée depuis l'extérieur soit sécurisée par un contrôle d'accès et au moyen d'un badge; les entrées fassent l'objet d'un procès-verbal; l'accès aux pièces dans lesquelles des données de la fondation sont traitées soit réservé aux seules personnes spécifiquement chargées de ce travail (need to know / least privileage).

Les mesures de sécurités sont déterminées par les zones protégées: les postes de travail sont protégés de l'intrusion de tiers; un système d'alarme est installé dans toutes les pièces.

Les pièces spéciales et les pièces telles que le centre de calcul et le «data-ware-house» sont protégées de la manière qui suit:

- le centre de calcul et tous les «data-ware-houses» / «data-center» / «data-server» sont sécurisés en adéquation avec leur catégorie de protection, laquelle implique des exigences de sécurités accrues et seules les personnes autorisées en charge de l'exploitation y ont accès;
- l'entrée fait l'objet d'un procès-verbal;
- le système d'alarme répond aux exigences de la catégorie de protection accrue;
- les serveurs se trouvent en sous-sol, dans des pièces de protection spécialement conçues à cet effet.

7.2 Contrôle des supports de données personnelles

Des mesures relevant de l'information assurent que seules les personnes autorisées peuvent traiter des données sur les supports de données électroniques. Seules les personnes autorisées ont accès aux fichiers et systèmes informatiques de la fondation ou de Swiss Life. Toutes les données doivent de plus être conservées sous clef et détruites de manière adéquate. Ceci empêche que des personnes non autorisées puissent lire, copier, modifier ou supprimer des supports contenant des données personnelles.

L'organisation interne de la fondation ou de tiers impliqués détermine les profils d'accès et les droits pour tous les collaborateurs. Ceux-ci sont régulièrement contrôlés.

Le collaborateur est tenu de s'identifier et de s'authentifier lors du lancement du système / de l'ordinateur portable. Cette procédure fait systématiquement l'objet d'un procès-verbal.

7.3 Contrôle des utilisateurs / Identification et authentification

Les droits d'accès dépendant d'un rôle, l'authentification et l'identification, les pare-feu de même qu'une réglementation claire en termes d'accès à distance contribuent à empêcher tout accès non autorisé aux données de la fondation.

La procédure d'identification d'une personne et d'authentification afférente passe par les étapes suivantes:

- l'accès aux systèmes de la fondation ou de Swiss Life est protégé par l'ID utilisateur, associé à un mot de passe individuel à durée de validité limitée et à la complexité adéquate, l'accès à certains systèmes requiert l'utilisation d'un mot de passe supplémentaire;

- l'utilisation des mots de passe est de plus soumise à une instruction spécifique et est régulièrement contrôlée;

- tous les comptes utilisateur permettant une authentification sont individuels, ainsi, il n'y a qu'un utilisateur par compte;

- tous les disques durs des collaborateurs sont en plus protégés par mot de passe;

- les mots de passe doivent être complexes et régulièrement modifiés (tous les 3 mois).

7.4 Contrôle de communication

Les destinataires de données, dont les données personnelles sont communiquées au moyen de dispositifs de transmission des données, sont identifiés via les interfaces et authentifiés de manière adéquate. De plus, les données sont envoyées aux postes définis par l'alinéa 5.4, généralement par correspondance.

7.5 Contrôle de mémoire

Des droits d'accès basés sur des rôles de même que la séparation des processus de test, de développement et de production empêchent qu'une personne non autorisée prenne connaissance, modifie ou supprime les données sauvegardées. Des antivirus et des pare-feu bloquent les logiciels malveillants et les accès externes non autorisés.

Les données sont archivées de manière à en assurer la révision.

7.6 Exigences techniques appliquées aux terminaux

Le traitement des données utilisateur ne passe par aucun terminal.

7.7 Contrôle d’accès

Seules les personnes dont les tâches quotidiennes - contribution aux objectifs de la fondation - requièrent l'accès aux données de la fondation peuvent y accéder.

7.8 Contrôle des saisies / procès-verbaux

Tous les systèmes disposent d'un traitement (accès aux données compris) consigné par procès-verbal. Ceci contribue tant à la protection de l'intégrité qu'au contrôle de l'affectation des données. Le procès-verbal est ainsi effectué en vertu de l'art. 10 OLPD. Les procès-verbaux sont conservés de manière professionnelle pour une durée déterminée. Seules les personnes en charge de surveiller et de veiller à l'application des prescriptions en matière de protection des données y ont accès, en adéquation avec l'affectation desdites données.

7.9 Développement de programmes

La séparation des processus de développement, de test et de production est maintenue.

7.10 Surveillance et responsabilité

Les propriétaires de l'information, conjointement avec les responsables d'application, veillent à ce que les personnes observent les instructions, le présent règlement de traitement et les dispositions.

7.11 Visiteurs dans les locaux de la fondation ou de tiers impliqués

La réglementation impose que les visiteurs s'annoncent préalablement et soient accompagnés lors de leurs déplacements dans les bâtiments. A l'entrée, l'identité des personnes est vérifiée au moyen d'une pièce d'identité, qui sera conservée au dépôt pendant leur visite.

7.12 Sécurité du poste de travail

La sécurité du poste de travail des collaborateurs est assurée par les mesures suivantes:

- les contenus de l'écran ne doivent pas être visibles par une tierce personne se tenant dans l'encadrure de la porte. Les postes de travail sont installés en conséquence;

- les collaborateurs reçoivent l'instruction - complétée par des formations régulières - de ne pas laisser des documents sans surveillance près de l'imprimante;

- une «Clean-Desk-Policy» clairement définie vaut pour tous les postes de travail, tous les documents doivent être conservés sous clef;

- les ordinateurs portables doivent être cadenassés aux postes de travail;

- tous les ordinateurs portables sont protégés par des pare-feu et des programmes antivirus, lesquels sont régulièrement mis à jour et correspondent au «state-of-the-art».

7.13 Accès en dehors de l'organisation

L'accès aux données de la fondation se fait uniquement au sein de l'organisation ou des locaux de tiers impliqués. Aucun support de données externe n'est employé pour le traitement de données de la fondation.

7.14 Protection durable des données

Les mesures de sécurité définie doivent être garanties pour toute la durée du cycle de vie, ce à quoi concourent les mesures suivantes:

- les données sont saisies uniquement par des personnes autorisées disposant de la formation adéquate;

- les données utilisées pour des tests sont, si possible, fictives ou anonymisées;

- la saisie, la modification, l'élimination et l'accès aux données font l'objet d'un procès-verbal rédigé de manière claire, uniquement destiné à assurer la sécurité et conforme à des critères clairs; les droits d'accès aux procès-verbaux sont clairement définis (need to know) et restreints à l'affectation déterminée; les procès-verbaux bénéficient des mêmes mécanismes de protection que les données (protection contre les accès non autorisés et les modifications);

- le contenu et la durée de conservation des fichiers de log correspondants sont en rapport avec les données et les mesures de traitement;

- l'archivage des données sur le long terme est conforme aux prescriptions du Code des obligations et de l'Olico. La suppression ou la destruction des données sont définies par une instruction spécifique.

7.15 Contrôle du transport

La transmission des données s'effectue via connexion VPN ou TLS. En général, les données ne sont pas envoyées aux personnes concernées par e-mail, mais par courrier.

8. Droits des personnes concernées

8.1 Droit à l'information

Chaque personne est en droit de savoir si la fondation ou Swiss Life traite des données la concernant. Dans ce contexte, le droit à l'information repose sur les dispositions de la LPD. Les requêtes doivent être déposées auprès de la fondation ou de Swiss Life SA, une pièce de légitimation officielle en annexe.

La procédure est définie par l'instruction sur la protection des données SLCH 8.13.

8.2 Obligation de fournir des informations pour les données sensibles

En vertu de l'art. 7a LPD, les personnes concernées doivent être informées lorsque des données sensibles sont traitées ou des profils de la personnalité établis à leur sujet.

De manière générale, les données personnelles sensibles ne peuvent être obtenues qu'avec l'accord de la personne concernée. Dans tous les autres cas, la règle d'exception selon l'art. 7a al. 4 s'applique, permettant la sauvegarde ou la diffusion des données en vertu du mandat légal.

8.3 Droit de rectification et d'effacement

Les personnes concernées par les droits de rectification et d'effacement se basent sur l'art. 5 alinéa 2 LPD en liaison avec l'art 25 LPD, les demandes doivent cependant être envoyées à la fondation.

9. Dispositions finales

9.1 Annexes

Les annexes mentionnées dans le présent règlement de traitement en font partie intégrante. Le règlement de traitement est géré et conservé par les responsables de la protection des données de Swiss Life.

9.2 Modifications apportées au règlement

L'état de mise à jour du règlement de traitement est régulièrement vérifié - et adapté si nécessaire. Les modifications doivent être faites sous forme écrite et sont soumises à l'approbation de la fondation. La fondation est responsable de la mise à jour.

9.3 Entrée en vigueur

Ce règlement, et toutes ses annexes entrent immédiatement en vigueur.

Zurich, le 29 septembre 2011

Fondation Caisse d'indemnités journalières pour artistes

Le président:

……

Stephan P. Thaler

Le trésorier:

……..

Adrian Steinmann

Annexe 1 – Catégories de données

Catégories auxquelles appartiennent les données personnelles dans le fichier:

Formule d'appel
Prénom
Nom
Entreprise
Numéro d'assuré (AVS)
Adresse1
Adresse 2
NPA
Lieu
Pays
N° de tél.
N° de fax
E-mail
Sexe
Langue
Numéro de partenaire (n° d'assuré)
Date de naissance
Date d'entrée
Date de sortie
Age de la retraite (calculé)
Décédé (oui/non)
Section
Style
Lieu de paiement: établissement financier, n° de compte
Admission sous réserve (oui/non)
N° du dommage (généré par le système)
Date de déclaration
Durée de - à
Description
Type (maladie/accident/congé maternité)
Cas classé (oui/non)
Cas de prestation en paiement de date à date
Délai de carence
Degré (en pourcent)
Montant de l'indemnité journalière (à titre informatif)
Indemnité journalière en CHF (à titre informatif)
Montant total en CHF

Indemnité journalière versé le date
Compte débiteur (information de comptage pour la comptabilité SAP)
Compte créditeur (information de comptage pour la comptabilité SAP)