

# Règlement sur la protection des données de SWICA

SWICA Organisation de santé (groupe SWICA, appelé ci-après SWICA) traite des informations relatives aux assurés dans le cadre de processus organisationnels complexes et pour lesquels il est fait appel à des équipements techniques de pointe. Ce règlement – dont le contenu découle du concept régissant le système de gestion de la protection des données de SWICA (W-3000) – définit la mise en œuvre de ce dernier au sein de l'entreprise. La position adoptée par SWICA en matière de protection des données est énoncée dans un document publié séparément sous le titre «*Politique de protection des données*» (il fait partie intégrante du document «*Gestion de la protection des données*»).

## Sommaire

	Page
1 But	2
2 Champ d'application	2
3 Bases juridiques dans le domaine de la protection des données	2
4 Concepts	2
5 Principes régissant le traitement des données	3
6 Autorisations d'accès	3
7 Transmission de données personnelles à l'interne	3
8 Transmission de données personnelles à l'extérieur	3
9 Droit de la personne concernée à consulter les dossiers et d'accéder aux données	3
10 Traitement de données personnelles par des tiers	4
11 Système d'information	4
12 Médecin-conseil	4
13 Conservation et destruction de données personnelles	4
14 Conseiller/ère à la protection des données en entreprise	4
15 Règlement sur le traitement des données de fichiers automatisés	4
16 Information et formation des collaborateurs	4
17 Responsabilité de la mise en œuvre et du respect de la protection des données	4
18 Entrée en vigueur	4

## 1 But

Le présent règlement sur la protection des données a pour objet la protection de la personnalité et des droits fondamentaux des individus lors du traitement de leurs données personnelles par les collaborateurs de SWICA Organisation de santé (groupe SWICA, appelé ci-après SWICA).

Ce règlement est applicable aux sociétés suivantes de SWICA: SWICA Assurance-maladie SA, SWICA Assurances SA, PROVITA Gesundheitsversicherung AG, ProVAG Versicherungen AG ainsi que SWICA Management AG.

Il fait partie intégrante du concept global de SWICA en matière de protection des données dont l'objectif est de sécuriser dans toute la mesure du possible les données personnelles sensibles.

## 2 Champ d'application

- 2.1 Les dispositions du présent règlement sur la protection des données sont applicables indépendamment du point de savoir si les données personnelles sont contenues sur des supports papier ou sont enregistrés électroniquement. De même, le fait qu'elles soient traitées manuellement ou via l'utilisation d'appareils électroniques est sans incidence.
- 2.2 Le traitement de données personnelles tirées de documents extérieurs publics accessibles à quiconque peut être effectué ouvertement.
- 2.3 La protection de la personnalité contre des atteintes illicites qui lui seraient portées est garantie sur le plan du droit civil de manière générale par le CC ou le CO.
- 2.4 Le présent règlement est applicable à tout traitement automatisé ou manuel de données se rapportant à des personnes physiques ou morales. Peu importe que ce traitement soit le fait de collaborateurs travaillant dans les secteurs d'activité de SWICA en tant qu'assureurs ou celui d'auxiliaires de SWICA ayant accès aux bureaux et archives, ou pouvant consulter des données personnelles.

## 3 Bases juridiques dans le domaine de la protection des données

Dans le domaine de l'assurance obligatoire des soins et de l'assurance-accidents, les dispositions prévues par la LPGA, la LAMal et la LAA priment les dispositions de la LPD, lesquelles s'appliquent à titre subsidiaire. Pour le surplus, les fondements légaux suivants entrent notamment en ligne de compte:

- Code civil suisse (CC) art. 27 ss.
- Code des obligations (CO) art. 328 (contrat de travail)
- Loi fédérale sur la protection des données (LPD)
- Ordonnance relative à la loi fédérale sur la protection des données (OLPD)
- Loi fédérale sur la partie générale du droit des assurances sociales (LPGA)
- Ordonnance sur la partie générale du droit des assurances sociales (OPGA)
- Loi fédérale sur l'assurance-maladie (LAMal)
- Ordonnance sur l'assurance-maladie (OAMal)
- Loi fédérale sur l'assurance-accidents (LAA)
- Ordonnance sur l'assurance-accidents (OLAA)
- Code pénal suisse (CP)

## 4 Concepts

### a. Données personnelles

Constituent des données personnelles toutes les informations qui se rapportent à une personne identifiée ou identifiable.

### b. Personne concernée

Est réputée concernée toute personne physique ou morale dont les données sont traitées.

### c. Données sensibles

Sont réputées sensibles les données personnelles sur les opinions ou activités religieuses, philosophiques, politiques ou syndicales, les données touchant la santé, la sphère intime ou l'appartenance à une race, ainsi que celles relatives à des mesures d'aide sociale, à des poursuites ou à des sanctions pénales ou administratives.

En particulier, les données suivantes peuvent contenir des informations sur la santé d'une personne:

- notes sur le déroulement d'un traitement
- descriptions de symptômes
- diagnostics
- ordonnances médicales
- rapports médicaux / rapports hospitaliers
- thérapies
- médicaments
- renvois
- résultats de laboratoire
- positions tarifaires
- notes sur des images médicales, etc.

### d. Profil de la personnalité

Un profil de la personnalité est un ensemble de données permettant de cerner les caractéristiques essentielles de la personnalité d'un individu en particulier.

e. *Traitement de données*

Constitue un traitement de données toute opération relative à des données personnelles, quels que soient les moyens et procédés utilisés. Sont concernés notamment la collecte, la conservation, l'exploitation, la modification, la communication, l'archivage ou la destruction de données.

f. *Communication*

Est réputé être une communication le fait d'ouvrir un accès à des données personnelles, par exemple en autorisant leur consultation, en les transmettant ou en les diffusant.

g. *Fichier*

Constitue un fichier tout ensemble de données personnelles dont la structure permet de rechercher les données par personne concernée.

h. *Organes fédéraux*

Les autorités ou services fédéraux ainsi que les personnes chargées d'une tâche de la Confédération sont des organes fédéraux. SWICA est réputée être un organe fédéral dans le cadre de l'assurance obligatoire des soins (LAMal) et de l'assurance-accidents obligatoire (LAA).

## 5 Principes régissant le traitement des données

- 5.1 Les données personnelles ne peuvent être traitées qu'à la condition qu'une disposition légale le prévoit ou que la personne concernée y consente. Dans l'assurance obligatoire des soins, les données relatives à la santé sont susceptibles d'être traitées en vertu de l'art. 84 LAMal. La communication de données à des tiers ne peut avoir lieu qu'aux organismes cités à l'art. 84a LAMal. Dans le domaine de l'assurance-accidents obligatoire, l'art. 96 s. LAA est applicable en la matière.
- 5.2 Les documents comportant des données relatives à la santé d'assurés sont traités uniquement dans les locaux de l'entreprise. Des exceptions à ce principe peuvent être accordées par le supérieur hiérarchique dans des cas justifiés (p.ex. home office), cela sous réserve de contrôles.
- 5.3 Dans le domaine de l'assurance complémentaire des soins (LCA), des données relatives à la santé peuvent être traitées pour autant que cela soit nécessaire à la mise en œuvre du contrat. Leur communication à des tiers est illicite sans une procuration de l'assuré.
- 5.4 Les données personnelles ne peuvent être traitées que pour le but tel qu'il est indiqué lors de leur collecte ou tel qu'il ressort des circonstances ou est prévu par une loi.
- 5.5 Dans le traitement de données personnelles, le principe de proportionnalité est à respecter. Ce dernier exige en particulier de ne recueillir que les données personnelles nécessaires et utiles à l'accomplissement des tâches (principe de la finalité).
- 5.6 La personne assurée doit être tenue au courant du traitement de ses données. En particulier, en cas de demande de communication de dossier, elle en sera informée (principe de transparence), à moins que ce renseignement ne nuise au but que vise la demande en question (p.ex. en cas de violation de l'obligation d'annonce) ou qu'il n'existe ni base légale ni accord de sa part.

## 6 Autorisations d'accès

Les collaborateurs de SWICA ont accès uniquement aux données personnelles dont ils ont besoin pour l'accomplissement de leur tâche. Les autorisations d'accès sont définies en conformité avec la loi.

## 7 Transmission de données personnelles à l'interne

- 7.1 Les collaborateurs sont autorisés à transmettre des données personnelles à l'interne pour autant que cette communication soit indispensable à l'accomplissement de leur tâche et que la mesure s'inscrive dans le but visé par la collecte des données. Le principe de proportionnalité est à respecter, à savoir que seules les données indispensables à la poursuite du but concret que vise leur traitement peuvent être transmises.
- 7.2 Des données personnelles sensibles ne doivent pas transiter via des réseaux de communication externes (e-mail, Internet), si ce n'est sous une forme cryptée.

## 8 Transmission de données personnelles à l'extérieur

- 8.1 La communication à l'extérieur de données personnelles ne peut avoir lieu qu'à destination d'organismes autorisés selon l'art. 84a LAMal ou l'art. 97 LAA. Dans le domaine de la LCA, elle ne saurait avoir lieu qu'en présence d'une procuration.
- 8.2 La transmission de données personnelles méritant protection ne peut avoir lieu via des réseaux de communication externes (e-mail, Internet), si ce n'est sous une forme cryptée.

## 9 Droit de la personne concernée à consulter les dossiers et d'accéder aux données

- 9.1 Les personnes assurées sont autorisées en vertu de la loi à consulter les données les concernant.
- 9.2 Le traitement des demandes d'accès fondées sur l'art. 8 LPD relève de la compétence du/de la conseiller/ère à la protection des données en entreprise. Il/elle rassemble les documents existants et les fait parvenir à la personne concernée.
- 9.3 Les informations selon l'art. 42 al. 5 LAMal, notamment les données relatives à la santé ayant un caractère stigmatisant ainsi que les indications médicales sans incidence pour le traitement des prestations, sont conservées exclusivement par le service du médecin-conseil. La demande de leur remise est effectuée directement par le/la conseiller/ère à la protection des données en entreprise.

## 10 Traitement de données personnelles par des tiers

Si le traitement de données personnelles est confié à un tiers, SWICA demeure responsable de la protection des données. L'entreprise veille, dans les limites de ses possibilités, à ce qu'elles soient traitées conformément au mandat et protégées contre un accès non autorisé (art. 22 OLPD).

## 11 Système d'information

- 11.1 SWICA conçoit et protège ses systèmes d'information de manière à ce que les services qu'elle fournit à ses assurés respectent comme il se doit les principes de la confidentialité, de l'intégrité, de la disponibilité et de la traçabilité des données (sécurité de l'information).
- 11.2 La directive «*Sécurité de l'information*» (W-4000) règle notamment ce qui suit dans la perspective de la protection des données:
- le contrôle de l'accès (droits d'accès, surveillance de l'accès, gestion de l'accès) des collaborateurs au système d'information ou aux données d'assurés;
  - la sécurité des données (back-up, archivage);
  - la sécurité du réseau (réseaux dignes de confiance, cryptage, protection du mot de passe, connexion à des entreprises tierces, accès Internet).
- 11.3 SWICA désigne à cette fin un responsable de la sécurité des systèmes d'information (CISO).

## 12 Médecin-conseil

SWICA organise un service de médecin-conseil conformément aux dispositions de l'art. 57 LAMal.

## 13 Conservation et destruction de données personnelles

- 13.1 L'ensemble des locaux abritant des données personnelles sont protégés contre un accès non autorisé.
- 13.2 Les données personnelles sont conservées conformément à la loi et protégées contre tout accès non autorisé.
- 13.3 La destruction de données personnelles sensibles sur support papier est confiée à un service spécialement créé à cet effet.
- 13.4 Les informations enregistrées sur des supports électroniques sont effacées de manière définitive avant l'élimination de ces derniers.

## 14 Conseiller/ère à la protection des données en entreprise

SWICA nomme en son sein un/e conseiller/ère à la protection des données en entreprise qui sera annoncé/e au Préposé fédéral à la protection des données et à la transparence (PFPDT).

Le/la conseiller/ère à la protection des données en entreprise veille au respect de la protection des données au sein de l'entreprise. En particulier, il/elle le fait lors de la conclusion de contrats et de la réalisation de projets, ainsi que pour ce qui a trait aux fichiers et à la formation des collaborateurs.

Il joue de rôle de personne de contact pour le Préposé fédéral à la protection des données et à la transparence et assure que les demandes d'accès au sens de l'art. 8 LPD soient satisfaites de manière correcte au niveau du fond et en temps utile.

## 15 Règlement sur le traitement des données de fichiers automatisés

Des règlements de traitement existent pour les fichiers automatisés selon l'art. 21 OLPD.

## 16 Information et formation des collaborateurs

Les collaborateurs sont régulièrement formés et instruits sur des sujets se rapportant à la protection des données et à la sécurité de l'information.

## 17 Responsabilité de la mise en œuvre et du respect de la protection des données

- 17.1 Les collaborateurs dans leur ensemble sont responsables du respect de la protection et de la sécurité des données pour leur domaine de compétence, cela dans le cadre des directives de SWICA.
- 17.2 La responsabilité générale en matière de protection des données incombe au conseil d'administration et à la direction générale selon leurs compétences respectives.

## 18 Entrée en vigueur

Cette directive entre en vigueur le 15 avril 2016 et remplace celle intitulée «*Règlement sur la protection des données SWICA*» (W-3100) du 8 juillet 2014.

Winterthour, le 15 avril 2016



Daniel Neuhaus  
Secrétaire général



Jérôme Egli  
Conseiller à la protection des données  
en entreprise