SWICA Data Protection Regulations

SWICA uses complex organisational processes and sophisticated technical facilities to store and process information about insured persons. These regulations are based on SWICA's data protection management system and govern the practical implementation of data protection at SWICA. SWICA's fundamental position on data protection is set out in its Data Protection Policy, which is published separately.

Contents

1 Purpose

The aim of these Data Protection Regulations is to safeguard the privacy and basic rights of individuals while employees of SWICA Healthcare Insurance Ltd, SWICA Insurance Ltd, PROVITA Health Insurance Ltd and ProVAG Insurance Ltd process their personal data.
These regulations are valid for the following SWICA companies: SWICA Healthcare Insurance Ltd, SWICA Insurance Ltd, PROVITA Health Insurance Ltd, ProVAG Insurance Ltd, and SWICA Management Ltd.
These Regulations form part of SWICA's comprehensive approach to data protection, which aims to ensure maximum security for particularly sensitive personal data.

2 Scope

2.1 The provisions of the Data Protection Regulations apply regardless of whether the personal data in question is in hardcopy or electronic form and whether it is processed manually or with the help of electronic devices.

2.2 Processing personal data obtained from generally available external publications is permitted as long as no changes are made.

2.3 Under civil law, the protection of personal privacy against unlawful infringement is provided in general terms by the Swiss Civil Code (ZGB) and the Code of Obligations (OR).

2.4 The regulations set out in this document apply to any automated or manual processing of the data of natural persons and legal entities by employees of all units of SWICA's insurance operations and to auxiliary staff who have access to offices and archives etc. or who may otherwise come into contact with personal data in the course of their work.

3 Legal basis for data protection

In the case of mandatory healthcare insurance and accident insurance, the provisions of ATSG and KVG/UVG take precedence over those of the DSG. In other words, the provisions set out in DSG are subsidiary. Otherwise the legal basis is provided by:

- Swiss Civil Code (ZBG) Art. 27 ff.
- Swiss Code of Obligations (OR), Art. 328 (contract of employment)
- Swiss Federal Act on Data Protection (DSG)
- Ordinance to the Data Protection Act (VDSG)
- Federal Act on the General Part of the Social Security Law (ATSG)
- Ordinance on the General Part of the Social Security Law (ATSV)
- Federal Health Insurance Act (KVG)
- Federal Health Insurance Ordinance (KVV)
- Federal Accident Insurance Act (UVG)
- Federal Accident Insurance Ordinance (UVV)
- Swiss Criminal Code (StGB)

4 Definitions

a. *Personal data*
Personal data is any information which is or can be associated with a particular person.

b. *Affected persons*
Affected persons are natural persons and legal entities whose data is processed.

c. *Particularly sensitive personal data*
Particularly sensitive personal data is data which relates to a person's religious, ethical, political or social views or activities, health, privacy, race, social assistance measures, administrative or criminal proceedings or sanctions.
The following types of data, in particular, may contain information about a person's health:
- Records of a course of treatment
- Descriptions of symptoms
- Diagnoses
- Doctors' prescriptions
- Medical reports / hospital reports
- Therapies
- Medication
- Referrals
- Laboratory results
- Rate positions
- Results of imaging processes etc.

d. *Personality profile*
A personality profile is a collection of data which can be used to evaluate key aspects of a natural person's personality.

e. *Processing*
Processing is any handing of personal data, regardless of the means and procedures used, including, in particular, the acquisition, retention, use, alteration, disclosure, archiving or destruction of data.

f. *Disclosure*
Disclosure is the act of making personal data accessible, for example by permitting access, transmission or publication.

g. *Data collection*
A data collection is a collection of personal data which is structured in such a way that data associated with individual affected persons can be identified.

h. *Federal bodies*
These are federal authorities/agencies and individuals entrusted with public duties on behalf of the Swiss Confederation. SWICA is deemed to be a federal body under the terms of the Federal Health Insurance Act (KVG) and the Federal Accident Insurance Act (UVG).

5 Processing principles

5.1 Personal data may be processed only in accordance with statutory provisions and if the affected person has given his/her consent. In the case of mandatory healthcare insurance, health-related data may be processed under Art. 84 KVG. Data may only be disclosed to the third parties specified in Art. 84a KVG. Art. 96 f. UVG applies in the case of mandatory accident insurance.

5.2 Documents containing the health data of insured persons may only be processed on company premises. Exceptions in well-founded individual cases (e.g. home-office) are approved and monitored by management.

5.3 In the case of supplementary healthcare insurance (VVG), health data may only be processed if such processing is necessary for the performance of the contract. It is not permitted to share this data with third parties without the authorisation of the insured person.

5.4 Personal data may only be used for the purpose communicated to the person concerned at the time it was obtained, as apparent from the circumstances at that time, or as prescribed by law.

5.5 The principle of proportionality must be observed when processing personal data. The principle of proportionality requires that only those elements of personal data which are necessary and appropriate for performing the task in question may be acquired (principle of specificity).

5.6 The insured person must be informed of the data processing. In particular, the insured person must be informed whenever documents are requested (principle of transparency) unless this would defeat the purpose of requesting them (e.g. suspected breach of notification obligations), there is a statutory basis for the action, or the insured person has given his/her consent.

6 Access rights

SWICA employees have access only to the personal data which they need for their work. Access rights are defined in compliance with the law.

7 Internal sharing of personal data

7.1 Every employee may share personal data internally to the extent necessary for their work and for the purpose for which it was acquired. The principle of proportionality must be observed; in other words, only the data that is necessary for the actual processing purpose may be shared.

7.2 Sensitive personal data may be transmitted only over external communication networks (e.g. email, the internet) in encrypted form.

8 External sharing of personal data

8.1 Personal data may only be shared externally with authorised persons as set out in Art. 84a KVG and Art. 97 UVG. In the case of VVG, sharing is possible only if there is a relevant power of attorney.

8.2 Sensitive personal data may be transmitted only over external communication networks (e.g. email, the internet) in encrypted form.

9 Affected person's right to review documents and access information

9.1 Within the relevant legal framework, insured persons are granted access to files containing data relating to them.

9.2 Requests for information under Art. 8 DSG are handled by the Operational Data Protection Officer. The officer gathers the available documents and sends them to the affected person.

9.3 Data in accordance with Art. 42 para. 5 KVG – in particular data on health issues that are of a stigmatising character and medical information that is of no relevance to benefits processing – is held exclusively with the medical examiner's office. The Operational Data Protection Officer must request such data from the medical examiner's office directly.

10 Processing of personal data by third parties

Even if the processing of personal data is delegated to third parties, SWICA remains responsible for data protection. To the extent possible, SWICA ensures that personal data is processed in accordance with instructions and protected against access by unauthorised persons (Art. 22 VDSG).

11 IT systems

11.1 SWICA designs and protects its IT systems in such a way that it can provide its service to insured persons while ensuring the confidentiality, integrity, availability and traceability of information (information security).

11.2 The directive on “Information security” (W-4000) ensures data protection in particular through:

- Controlling employee access to IT systems and/or the data of insured persons (access rights, monitoring and management);
- Backing up and archiving data;
- Implementing network security (trusted networks, encryption, password-protection, links to other companies, internet access).

11.3 To this end, SWICA appoints a Chief Information Security Officer (CISO).

12 Medical officer

SWICA organises its Medical Examiner’s Office in accordance with the provisions set out inArt. 57 KVG.

13 Storage and deletion of personal data

13.1 All premises in which personal data is stored are protected against unauthorised entry.

13.2 Personal data is stored in accordance with relevant statutory requirements and protected against unauthorised access.

13.3 Particularly sensitive personal data held in hardcopy form is disposed of securely by a service specialising in this activity.

13.4 Information held on electronic storage devices is permanently erased prior to disposal.

14 Operational Data Protection Officer

SWICA appoints an Operational Data Protection Officer who is registered with the Federal Data Protection and Information Commissioner (FDPIC).

The Operational Data Protection Officer ensures that data protection regulations are observed at SWICA, especially in the drafting of contracts, in projects, in relation to data collections and in the context of employee training.

He/she is the point of contact for the Federal Data Protection and Information Commissioner and ensures that requests for information within the meaning of Art. 8 DSG are correct in terms of their content and are processed in a timely manner.

15 Processing regulations for automated data collections

Processing regulations, as set out in Art. 21 VDSG, exist for automated data collections.

16 Information and training for employees

Employees receive regular training and instruction on the topics of data protection and information security.

17 Responsibility for implementation and compliance

17.1 All employees are responsible for complying with data protection and data security regulations within their area of responsibility in accordance with SWICA directives.

17.2 Overall responsibility rests with the Executive Committee and the Board of Directors.

18 Entry into force

This directive enters into force on 15 April 2016 and replaces the directive “SWICA Data Protection Regulations” (W-3100) of 8 July 2014

Winterthur, 15.04.2016

Daniel Neuhaus
General Secretary

Jérôme Egli
Operational Data Protection Officer