DATA PROTECTION

PROCESSING REGULATIONS FOR SWICA'S AUTOMATED DATA COLLECTIONS.

BECAUSE HEALTH IS EVERYTHING SWICA

TABLE OF CONTENTS.

PROCESSING REGULATIONS FOR SWICA'S AUTOMATED DATA COLLECTIONS.

1. LIST OF ABBREVIATIONS

CEO	Chief Executive Officer
Dept.	Department
DRG	Diagnosis-Related Groups
DSG	Swiss Federal Act on Data Protection of 19 June 1992
DSV	Ordinance of 31 August 2022 on Data Protection
EMA process	Process by which employees join, leave or move within the company
FDPIC	Federal Data Protection and Information Commissioner
ICS	Internal control system
IT	Information technology, generic term for information and data processing
KVG	Federal Health Insurance Act of 18 March 1994
MEO	Medical Examiner's Office
SHP	Swiss Health Platform
UVG	Federal Accident Insurance Act of 20 March 1981
VVG	Federal Insurance Contract Act of 2 April 1908

2. GENERAL

2.1 LEGAL BASIS

In its role as federal body, SWICA Healthcare Organisation (SWICA Group, hereinafter referred to as "SWICA") processes personal data within the meaning of the Data Protection Act in the context of the Health Insurance Act (KVG) and the Accident Insurance Act (UVG). It also processes personal data of this kind as a private legal entity under the Insurance Contract Act (VVG).
Pursuant to Articles 5 and Art. 6 of the Ordinance on Data Protection (DSV), SWICA is required to produce processing regulations for its automated data collections.

2.2 PURPOSE OF THE PROCESSING REGULATIONS

The purpose of these regulations is to provide the necessary transparency regarding automated data processing at SWICA. In particular, it provides information about:

- the IT structure and the data collections contained therein.
- data processing processes.
- third parties involved in the data collections.
- the origin, access to and sharing of the personal data processed in the data collections.
- the procedure for exercising the right to information.

2.3 SCOPE OF APPLICATION OF THE PROCESSING REGULATIONS

These regulations apply to the automated data collections of the SWICA IT structure as used by the following companies within the SWICA Healthcare Organisation:

- SWICA Healthcare Insurance Ltd
- SWICA Insurances Ltd
- SWICA Management AG

The processes used for processing data are identical at all the listed companies.

2.4 RESPONSIBILITY

The Executive Committee of SWICA is responsible for the insurance business which the company operates and is therefore the owner of the data collections.

2.5 PURPOSE OF THE DATA COLLECTIONS

SWICA maintains data collections in order to fulfil its obligations as a health, accident, daily benefits and supplementary insurer within the statutory or contractual framework.

2.6 DATA PROTECTION CONSULTANT

SWICA has a Data Protection Consultant within the meaning of Art. 10 DSG in conjunction with Art. 25 et seq. DSV.

3. SWICA'S IT STRUCTURE

3.1 OVERVIEW

SWICA's core and peripheral systems are used to carry out activities as part of both mandatory health insurance (KVG) and supplementary insurance (VVG). SWICA uses the services provided by Centris AG, which offers an integrated solution in the form of the Swiss Health Platform (SHP). SWICA also uses other applications to supplement the services provided by Centris AG.
SWICA maintains a record of its processing activities in accordance with Art. 12 DSG. The record of processing activities also contains the list and description of the individual components and interfaces (see also Register of processing activities – FDPIC).

3.2 RESPONSIBILITIES

Technical responsibility for the individual core applications lies with SWICA's application owners.

4. TECHNICAL AND ORGANISATIONAL CONTROLS (TOC)

4.1 GENERAL

SWICA operates an Information Security Management System (ISMS) based on ISO 27001. The technical and organisational measures taken by SWICA include the following:

4.1.1 Access control

SWICA's premises are electronically secured to prevent access by unauthorised individuals. Access to rooms in which particularly sensitive data is held or processed is additionally restricted to the necessary group of employees.

4.1.2 Data medium control

Unauthorised individuals are prevented by technical means from reading, copying, modifying or deleting data, for example through data encryption, secure storage of data carriers or proper destruction.

4.1.3 Transmission control

Data which is transmitted over the network is protected. To this end, SWICA uses private and encrypted communication channels. All external storage devices must be fitted with an encryption mechanism.

4.1.4 Disclosure control

Partners who are linked to the encrypted network are known and uniquely identified. Technical means are used to ensure that unknown institutions and individuals cannot gain access to SWICA's networks.

4.1.5 Storage control

Unauthorised individuals are prevented by technical means from reading, copying, modifying or deleting data. Authorisation concepts ensure that employees only have access rights to the storage media that they require for their work (need-to-know principle).

4.1.6 User control

Authorisations are granted in accordance with SWICA's authorisation concept.

4.1.7 Access control (systems)

Authorisation concepts ensure that employees only have access rights to the data that they require for their work (need-to-know principle).

4.1.8 Input control (logging/log files)

Changes to personal data are archived. This information ensures the traceability of data processing.

5. INDIVIDUALS INVOLVED IN THE DATA COLLECTIONS

The employees, particularly at head office, together with the decentralised units (i.e. regional, general agencies and other agencies), are responsible for managing the insurance business.
Responsibilities in relation to data processing are governed in internal policies.

6. DATA PROCESSING

6.1 PURPOSE OF DATA PROCESSING

SWICA processes data exclusively for the purpose of conducting its insurance business, specifically, to document insurance relationships, evaluate applications, process benefits and payments, maintain statistics and provide information.

6.2 ORIGIN OF THE DATA

The data comes from the insured persons themselves as well as from individuals and organisations (e.g. service providers, insurers and the authorities) which are entitled by law (in the case of mutual and administrative assistance) or authorised by the insured persons to provide SWICA with the data.

6.3 DATA SHARING

Data is shared in accordance with statutory provisions (Art. 84a KVG, Art. 97 UVG). In cases in which SWICA is not authorised/required by law to share information, data is shared with third parties only with the written consent of the person affected.

6.4 FURTHER INFORMATION

Further information on data processing can be found in SWICA's data privacy statement (Data Privacy Statement).

6.5 CONFIDENTIALITY AND PROFESSIONAL SECRECY OBLIGATIONS

6.5.1 Swica employees

In order to fulfil their responsibilities, SWICA employees process personal data, including particularly sensitive personal data, in SWICA's IT system.

SWICA employees sign a contract of employment in which they undertake to treat information discreetly and confidentially and to comply with data protection law.

To take account of the particular sensitivity of some classes of medical information, employees who report to the Medical Examiner's Office also sign a data protection and professional confidentiality declaration.

6.5.2 External partners

Cooperation agreements exist between SWICA and its external partners. The partners commit themselves contractually to ensuring that they, their employees and their auxiliaries to the same extent comply with the data protection provisions as they apply to SWICA employees.

6.6 DOCUMENTATION OF PROCESSES

SWICA's data collections are used in a variety of workflows. The individual processes are documented by the departments responsible for them.

6.7 DATA STORAGE AND DELETION

Data which must be archived is stored accordingly for the period specified by Swiss law and protected against modification and unauthorised access.

When the retention period ends, it is deleted from SWICA's IT system or destroyed.

7. AFFECTED PERSONS' RIGHT TO INFORMATION

Every person may exercise their rights under the Data Protection Act in respect of SWICA. To do so, the persons concerned must apply in writing and include a copy of an official identity document to the following address:
SWICA Healthcare Organisation
Data Protection Unit
Römerstrasse 37
8401 Winterthur
datenschutz@swica.ch

SWICA will check the request and grant the rights provided there is no legitimate reason to restrict the rights under the Data Protection Act.

8. PROJECT PLANNING, OPERATIONS, AND QUALITY MANAGEMENT

8.1 PROJECT PLANNING

Planned automated processing activities in the area of health and accident insurance are reported to the FDPIC at the time of the project development decision or of the project release in accordance with Art. 31 para. 1 DSV.

8.2 OPERATIONS

The operational features of the various core and peripheral systems are documented in manuals by the units responsible.

8.3 QUALITY MANAGEMENT

Quality assurance and enhancement for the various core and peripheral systems in SWICA's IT system are dealt with in a separately regulated internal control system (ICS).
The specialist process which bears responsibility for efficient and effective data processing and for compliance with the data protection regulations regularly verifies the effectiveness of the processes and defines test criteria. The Operational Data Protection Consultant is involved directly in defining the key figures in relation to data protection.
Internal audits are conducted on a regular basis where necessary and appropriate. Further internal audits are primarily carried out by Internal Audit.

9. FINAL PROVISIONS

9.1 FURTHER INFORMATION

These processing instructions contain basic information. In order to protect systems, processes and data, preserve the confidentiality of insured persons and safeguard the business secrets of SWICA and its business partners, no specific information will be published.

9.2 CHANGES TO THESE REGULATIONS

The Processing Regulations are reviewed regularly to ensure that they remain up to date. They can be amended at any time in accordance with the applicable provisions.

Winterthur, 1 September 2023
Version 3.1

Dr. oec. Reto Dahinden
CEO

Jérôme Egli
Data Protection Consultant

120e / online / 12.2024