Processing Regulations for SWICA's Automated Data Collections

SWICA, Römerstrasse 38, 8401 Winterthur

Table of contents

		Page
1	General	3
1.1	Legal basis	3
1.2	Purpose of the regulations	3
1.3	Scope of application of the regulations	3
1.4	Responsibility	3
1.5	Purpose of the data collections	3
1.6	Registration of the data collections with the FDPIC	3
2	SWICA's IT structure	4
2.1	Overview	4
2.2	Responsibilities	5
2.3	Interfaces	6
3	Technical and organisational controls	6
3.1	Access control	6
3.2	Control of storage media	6
3.3	Transmission control	6
3.4	Disclosure control	7
3.5	Storage control	7
3.6	User control	7
3.7	Access control	7
3.8	Input control (logging / log files)	7
4	Individuals involved in the data collections	7
4.1	SWICA employees	7
4.2	External agents / outsourcing	8
5	Data processing	8
5.1	Purpose of data processing	8
5.2	Origin of the data	8
5.3	Data categories	8
5.4	Data sharing	8
5.5	Confidentiality and professional secrecy obligations	8
5.5.1	SWICA employees	8
5.5.2	External partners	8
5.6	Documentation of processes	9
6	Data storage and deletion	9
7	Affected persons' right to information	9
8	Project planning, operations, and quality management	9
8.1	Project planning	9
8.2	Operations	9
8.3	Quality management	9
9	Final provisions	9
9.1	Further documentation	9
9.2	Changes to these regulations	9
9.3	Entry into force	9

List of abbreviations

CEO	Chief Executive Officer
Dept.	Department
DRG	Diagnosis Related Groups (rate system for in-patient acute somatic hospital services)
DSG	Swiss Federal Act on Data Protection of 19 June 1992
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
KVG	Federal Health Insurance Act of 18 March 1994
SHP	Swiss Health Platform
UVG	Federal Accident Insurance Act of 20 March 1981
MEO	Medical Examiner's Office
VDSG	Ordinance to the Data Protection Act of 14 June 1993
VVG	Federal Insurance Contract Act of 2 April 1908

1 General

1.1 Legal basis

In its role as federal body, 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 11 and 21 of the Ordinance to the Data Protection Act (VDSG), SWICA is required to produce processing regulations for its automated data collections.

1.2 Purpose of the regulations

The purpose of these regulations is to provide transparency regarding SWICA's data system and the data processed in it. 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 and sharing of the personal data processed in the data collections
- the procedure for exercising the right to information

1.3 Scope of application of the regulations

These regulations apply to the automated data collections of the SWICA IT structure as used by all companies within the SWICA Healthcare Organization ("SWICA"):

- SWICA Healthcare Insurance Ltd
- SWICA Insurances Ltd
- PROVITA Health Insurance Ltd
- ProVAG Insurance Ltd

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

1.4 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.

1.5 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.

1.6 Registration of the data collections with the FDPIC

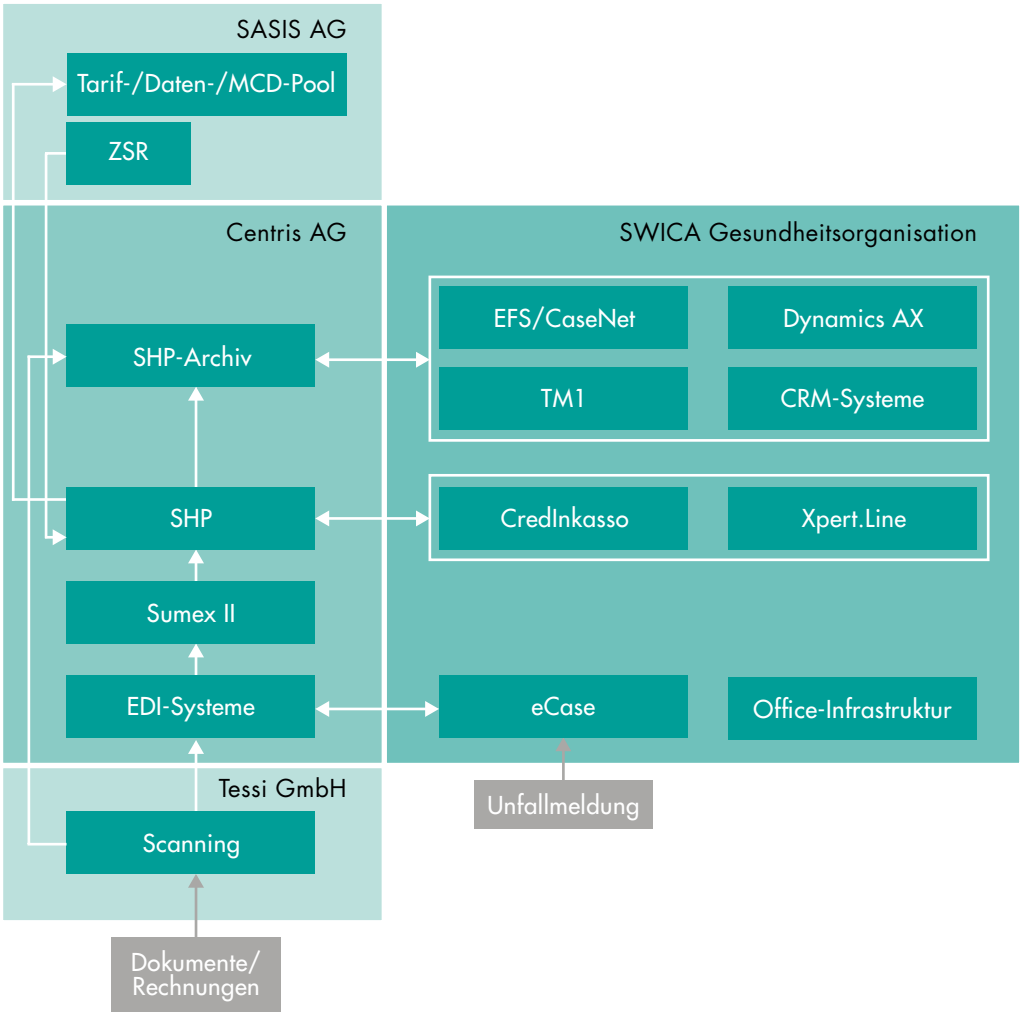
SWICA has an Operational Data Protection Officer within the meaning of Art. 11a para. 5 let. e DSG in conjunction with Art. 12a VDSG. SWICA is therefore not obliged to register its data collections with the Federal Data Protection and Information Commissioner (FDPIC).

2 SWICA's IT structure

2.1 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.

Overview of core applications:



Components	Description
SHP	Main system for processing insurance business in the private and corporate sectors
SHP Archive	Document archive for secure long-term storage of client data and policies
EDI systems	Electronic data interchange
Sumex II	Automated invoice checking
Scanning	Automated digitalisation of invoices and documents
EFS / CaseNet	Electronic case management system
Dynamics AX	SWICA accounting system
TM1	Data analysis
CRM systems	Sales systems for new clients, information systems for health advice (Achilles)
CredInkasso	Debt collection system for managing collection cases
Xpert.Line	Personnel system
eCase	Electronic case notification via secure web
Office infrastructure	Technologies for workstations, email, storage, data backups
Pool for rates / data / MCDs	Data analyses
PAR	Service provider data

2.2 Responsibilities

Technical responsibility for the individual core applications lies with the application owners in SWICA's IT department.
An internal list of the individual data collections held by SWICA (including the applications and databases in SWICA's IT system) is maintained by the Operational Data Protection Officer. This list provides specific information about the department responsible internally, the information flow (interfaces), and the appropriateness, specificity, proportionality and retention period for each data collection.

2.3 Interfaces

Unless otherwise noted, the interfaces documented here are automated data flows which are processed electronically.

From	To	Purpose	Data
Invoice	Scanning	Processing of invoices from service providers	Invoice data
Scanning	EDI systems	Automated processing of invoices	Electronic invoices
EDI systems	Sumex II	Invoice checking	Electronic invoice data
Sumex II	SHP	Invoice processing	Electronic invoice data
SHP	SHP Archive	Statutory archiving of client data	Benefit statements, business cases
EDI systems	eCase	Enable accident notifications for companies	Contract data for corporate clients
eCase	EDI systems	Case notifications for daily benefits and accident	Electronic accident notifications
SHP	CredInkasso	Collection cases	Debt collection information
CredInkasso	SHP	Statement checking	Payment data and collection statuses
SHP	Xpert.Line	Distribution partner statements	Commissions data for distribution partners
Xpert.Line	SHP	Distribution partner statements	Master data for personnel and intermediaries
SHP Archive	EFS / CaseNet	Processing of Managed Care patients after consent has been obtained from the client	Master and insurance data of approved cases
SHP Archive	EFS / CaseNet	Handling of recourse cases, objections and complaints	Corresponding case-related data
SHP Archive	TM1	Premium calculation and profitability reports	Expenditure per region
SHP Archive	Dynamics AX	Bookkeeping, financial accounting and cost accounting	Premiums, benefits, provisions, actuarial reserves
SHP Archive	CRM systems	Information for supporting existing clients	Master data and up-to-date insurance coverage
SHP	Pool for rates / data / MCD	Analyses that include cost-effectiveness checks and rate setting	Anonymised data on insured persons as per ISAK definitions

3 Technical and organisational controls

3.1 Access control

SWICA's premises are electronically secured to prevent access by unauthorised individuals (access is possible only using a key or badge). Access to rooms in which particularly sensitive data is held or processed (e.g. Medical Examiner's Office, server rooms) is additionally restricted to the necessary group of employees.
Measures (e.g. automatic activation of screen locking or the use of screen privacy filters at highly sensitive workstations) have also been implemented.

3.2 Control of storage media

Unauthorised individuals are prevented by technical means from reading, copying, modifying or deleting data. This is achieved through the authorisation process which ensures that employees can access only the data they need for their work.

3.3 Transmission control

Data which is transmitted over the network is protected. To this end, SWICA uses private encrypted communication channels. Data is not transmitted via the internet. Email communication between partners is also encrypted using a Switzerland-wide encrypted network. All external storage devices must be fitted with an encryption mechanism.

3.4 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 these networks.

3.5 Storage control

Unauthorised individuals are prevented by technical means from reading, copying, modifying or deleting data. This is achieved through the authorisation process which ensures that employees only have access to the storage media that they need for their work.

3.6 User control

User control is based on the EMA process by which employees join, leave or move within the company. New authorisations are not granted until and unless an individual's rights to access data have been checked and confirmed by two people. Existing rights are reviewed on a regular basis and amended as necessary. Employees who leave the company are prevented from accessing client and SWICA data after their last day at work (or sooner in some cases).

3.7 Access control

Employees only have access rights to the data they require for their work. The EMA process regulates the way in which employees join, leave or move within the company. In the case of internal moves, access rights which are no longer required are deleted from the systems; when individuals leave the company, all access rights are deleted.

A user name and password are required to access SWICA IT systems. Applications with sensitive personal data are additionally password-protected. Access rights within applications are limited to groups of employees. At employee level, access rights are issued on the basis of the role concept and in accordance with the "need-to-know" principle.

3.8 Input control (logging / log files)

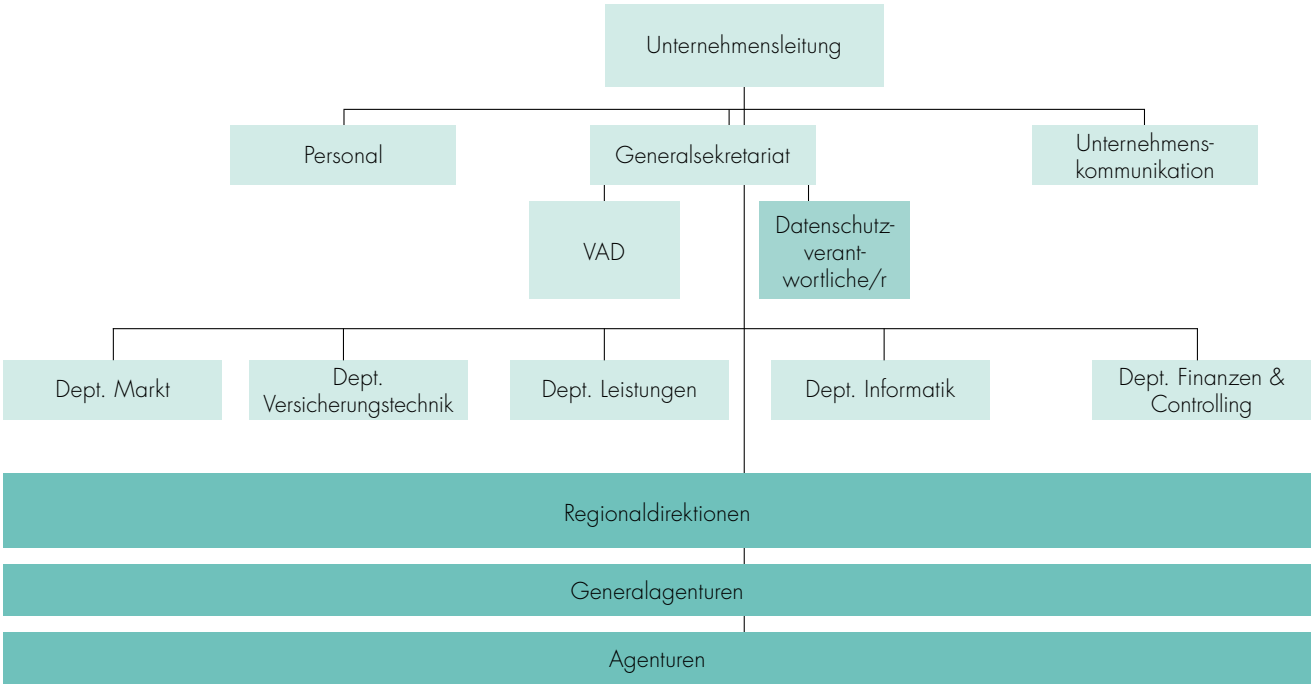
The SHP core system and all the main peripheral systems log changes to client data. These are then archived. This means that it is possible at any time to find out which employee changed which data.

Other log files relating to the network and to system access are available for tracking any irregularities.

4 Individuals involved in the data collections

4.1 SWICA employees

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.



4.2 External agents / outsourcing

Company	Contract	Core applications
Centris AG, Solothurn	Service contract with SLA	SHP, SHP Archive, Sumex II, EDI systems
Tessi GmbH, Urdorf	Service contract with SLA	Scanning
Aspectra AG, Zurich	Service contract with SLA	CaseNet
SASIS AG	Data delivery contract	SHP, pool for rates / data / MCD

5 Data processing

5.1 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.

5.2 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.

5.3 Data categories

The following data categories are processed in the relevant applications and protected against unauthorised access by the means mentioned above:

- Surname, first name, address, phone numbers
- Date of birth
- Nationality, language
- Family circumstances
- Legal representation, family members
- Information about illness / accident
- Health
- Social assistance measures
- Policy no.
- Social insurance number
- Benefits data
- Premium data
- Bank details
- Reminder data

5.4 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.

5.5 Confidentiality and professional secrecy obligations

5.5.1 SWICA employees

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

SWICA places a high priority on data privacy, is fully compliant with data protection law, and has issued the Data Protection Regulations, which are publicly available. 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.

5.5.2 External partners

Cooperation agreements exist between SWICA and its external partners. In these agreements, SWICA's partners undertake to ensure that their employees comply with the data protection regulations in the same way as SWICA employees.

5.6 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. Detailed documentation exists in particular for processes involving particularly sensitive personal data and personality profiles (DRG data receiving unit, processing of medical data in the MEO etc.).

6 Data storage and deletion

Data which must be archived is stored 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 can ask SWICA whether it has processed or is processing his or her personal data. To use this right to access information, the person must submit a written request to:
SWICA Healthcare Organisation
Data Protection Unit
Römerstrasse 38
8401 Winterthur
SWICA will check whether it has on its systems any data within the meaning of Art. 8 ff. DSG and, if so, will send a copy of it to the applicant within 30 days.

8 Project planning, operations, and quality management

8.1 Project planning

Project planning and implementation for the various core and peripheral systems in SWICA's IT system are governed by SWICA project guidelines. The project planning documentation is stored centrally.

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 Officer is involved directly in defining the key figures in relation to data protection.
Internal audits are conducted regularly. The audit reports form part of SWICA's corporate governance reporting which is presented to the Executive Committee and the Board of Directors as part of SWICA's approach to corporate governance.

9 Final provisions

9.1 Further documentation

These Processing Regulations reference a number of other documents. 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, these documents are not published.

9.2 Changes to these regulations

The Processing Regulations are reviewed regularly to ensure that they remain up to date. They can be changed at any time with the approval of the Executive Committee.

9.3 Entry into force

These regulations replace those of 1 September 2014 and enter into force on 15 April 2016.

Winterthur, 15 April 2016

Dr Reto Dahinden
CEO

Jérôme Egli
Operational Data Protection Officer