

SWICA ONLINE SERVICES

GENERAL TERMS AND CONDITIONS (T&CS) FOR ONLINE ACCESS TO SWICA ONLINE SERVICES.

TABLE OF CONTENTS.

I. General	3	VIII. Foreign legal systems/ import and export restrictions	7
II. Legal information	3	IX. Intellectual property	7
2.1 Conditions of use	3	X. Warranty and liability	7
2.2 Amendment of the T&Cs	3	XI. Fees and charges	7
III. Services	3	XII. Applicable law and place of jurisdiction ...	7
IV. Online access	3	XIII. Final provisions	7
4.1 Access rights	3		
4.2 Registration and login	3		
V. Duties of the User to exercise care	4		
VI. Security warnings/ Blocking and termination	4		
6.1 Security warnings	4		
6.2 Blocking online access	5		
6.3 Termination of online access	5		
VII. Data protection and use of data	5		
7.1 Control	5		
7.2 Purpose of data processing	5		
7.3 Data usage	6		
7.4 Logs and analysis	6		
7.5 Disclosure to third parties	6		
7.6 Retention	6		
7.7 Data security	6		
7.8 Rights of data subjects	6		

GENERAL TERMS AND CONDITIONS (T&CS) FOR ONLINE ACCESS TO SWICA ONLINE SERVICES.

I. GENERAL

SWICA Healthcare Insurance Ltd. (acting for all group companies of SWICA Healthcare Organisation, in particular SWICA Insurances Ltd. and SWICA Management Ltd, referred to below as «SWICA») offers secure and easy-to-use online access to its online services («Services») to customers who have a legal relationship with SWICA («Users» or «User»). These General Terms and Conditions for Online Access («T&Cs») govern the relationship between SWICA and the User in connection with registration and login for the Services.

The distributor is SWICA Healthcare Insurance Ltd., Römerstrasse 38, 8400 Winterthur, UID CHE-109.337.400.

The technology provider is Ergon Informatik Ltd., Merkurstrasse 43, 8032 Zurich.

The operator is Aspectra AG, Weberstrasse 4, 8004 Zurich.

II. LEGAL INFORMATION

2.1 CONDITIONS OF USE

Some Services provided by SWICA require an additional agreement, which must be agreed separately in the relevant service. By registering for the Services, the User accepts these T&Cs.

2.2 AMENDMENT OF THE T&CS

SWICA explicitly reserves the right to amend these General Terms and Conditions at any time. Any such amendment will be communicated to the User electronically and must be accepted when the User next logs in, otherwise the customer's right to use the Services will lapse.

III. SERVICES

The Services include mySWICA, BENEVITA, BENECURA and Compassana. SWICA may change (i.e. reduce or expand) the offering of Services at any time or end access to them completely.

IV. ONLINE ACCESS

4.1 ACCESS RIGHTS

It is not permitted to open accounts for third parties, except in the case of minors or adults under guardianship.

4.2 REGISTRATION AND LOGIN

Registration requires:

- › An active insurance relationship with SWICA on the day of registration
- › Own email address
- › Own mobile telephone number

To obtain online access, the User must register at idp.swica.ch/auth. If the registration process is interrupted before a second authentication factor can be set up, the process must be started again for security reasons. In addition to the user name and personal password, registration requires a second means of authentication (two-factor authentication). Customers can select from the following options:

- › One-time password (OTP) via text message (SMS) (you may be charged to receive text messages)
- › External security key in accordance with the FIDO (Fast Identity Online) standard

Users can choose between these authentication factors. FIDO also enables passwordless two-factor authentication. Please note that authentication via FIDO is regarded as more secure than SMS authentication.

Customers can also activate biometric login for the various Services at their own risk. If this is activated, customers can alternatively verify their identity using the biometric authentication on their device (e.g. fingerprint or facial recognition).

V. DUTIES OF THE USER TO EXERCISE CARE

SWICA draws the User's particular attention to the following obligations to exercise due care when using the Services:

- › The User must ensure that access data is kept secret and protected against misuse by unauthorised persons. Passwords must not be written down, shared or stored without protection on the end device. Passwords must not be easy to guess or otherwise ascertain.
- › If there is reason to suspect that unauthorised third parties are aware of the password, the password must be changed immediately and, if necessary, a request sent to SWICA to block access.
- › Where FIDO is used, the customer is obliged to keep the list of FIDO devices up to date in the SWICA credentials manager. In the event of theft, loss or transfer of a FIDO device, the customer is obliged to deactivate or remove the device in the SWICA credentials manager or to report the loss to SWICA.
- › In the event of a change to personal data such as email address (login username) and mobile number (2FA), the customer is obliged to amend this data immediately, assuming they are able to log in. Otherwise they must report the change to SWICA.
- › There must be no infringement of industrial property rights, copyrights or other proprietary or/intellectual property rights. SWICA explicitly reserves the right to take legal action if it finds that the User has infringed intellectual property rights or other copyright. In any event, SWICA will cooperate fully with the authorities.
- › The customer is obliged to take the necessary security precautions to prevent unauthorised access by a third party or the installation of malware on devices used to access the aforementioned Services. SWICA accepts no liability for any loss or damage caused by modifications to the operating system such as jailbreaking, rooting, or bypassing, omitting or ignoring security features.

The User bears all risks arising from the infringement of the aforementioned duties to exercise care.

VI. SECURITY WARNINGS/BLOCKING AND TERMINATION

6.1 SECURITY WARNINGS

Access to the Services is provided online via an internet service provider selected by the customer. The web application is optimised for current versions of commonly used browsers. Some functions may not work properly when using older versions or less common browsers. The Services run on all modern smartphones with up-to-date iOS or Android operating systems. Some functions may not work properly when using older devices or operating system versions. Despite state-of-the-art security precautions, it is not possible to guarantee absolute security either on SWICA's side or on the User's side. The User's terminal device is part of the internet and is outside SWICA's control. SWICA draws the User's particular attention to the following risks when accessing the Services:

- › Inadequate system knowledge and security precautions on the terminal device may allow unauthorised access to customer data. SWICA therefore strongly recommends that Users equip their terminal devices with up-to-date protection programs and run all programs and systems at the maximum possible security level. Users are advised not to use a public or unknown WLAN to access the Services.
- › If there is any suspicion that unauthorised third parties have become aware of the access data, it must be changed without delay and, where necessary, SWICA must be asked to block access.
- › SWICA has no influence on whether or how the internet provider selected by the User analyses data traffic. If there is no activity on the Services for a defined period of time, the current session will be terminated automatically for security reasons and the User will have to log in again. There is a latent risk that a third party may gain access to the User's terminal device while Services are being used without the User being aware that this is the case.
- › When using a network (e.g. the internet, SMS, WLAN), there is a risk that malware or similar could infect the terminal device when it is connected to the network. Appropriate security software available on the market can assist Users with their security precautions.
- › Despite the use of state-of-the-art security technologies, there can be no guarantee of absolute security in the context of data transmission.

- › The data can be transmitted uncontrolled across borders. This also applies even if both the sender and the receiver are located in Switzerland. Although the individual data packets are transmitted in encrypted form, the senders' and recipients' details are unencrypted. It is therefore possible to infer a customer relationship between the User and SWICA.

SWICA rejects all liability for the consequences of non-compliance with the security warnings.

6.2 BLOCKING ONLINE ACCESS

SWICA reserves the right to block online access if these conditions of use or the conditions of use of a specific service are breached, or if a security risk is identified.

6.3 TERMINATION OF ONLINE ACCESS

Online access will be terminated

- › if the User no longer has a contractual relationship with SWICA.
- › if the User deletes their own online access.
- › if the business administrator deletes the online access (see section 6.2).
- › if the User has not accessed the service for three years.

It is the User's responsibility to save, outside the Services, all data and documents that they wish to keep after the end of the contract.

VII. DATA PROTECTION AND USE OF DATA

7.1 CONTROL

SWICA controls the collection of data. The company can be contacted at the following address:

SWICA Healthcare Insurance Ltd.

Data Protection

Römerstrasse 38

8401 Winterthur

Contact details for Liechtenstein:

SWICA Vaduz Administrative Office

Meierhofstrasse 2

9490 Vaduz

Email: datenschutz@swica.ch

7.2 PURPOSE OF DATA PROCESSING

SWICA processes data during registration and login. SWICA uses the personal data it collects only for the purpose of providing online access to enable use of the Services.

SWICA complies with the relevant laws when handling personal data.

In Switzerland, these are:

- › The Federal Act on Data Protection of 25 September 2020 (DSG)
- › Ordinance of 31 August 2022 on Data Protection (DSV)

In Liechtenstein, these are:

- › Data Protection Act issued on 7 December 2018 (DSG; referred to below as DSG II)
- › Data Protection Ordinance issued on 19 December 2018 (DSV; referred to below as DSV II)
- › General Data Protection Regulation of the European Parliament and of the Council of 27 April 2016 (GDPR)

In particular, SWICA does not share personal information about Users with third parties unless authorised to do so and protects the personal data entrusted to it against unauthorised access by taking appropriate technical and organisational measures.

SWICA's executive bodies, employees and agents are legally obliged to maintain confidentiality with regard to Users' personal data and business documents.

7.3 DATA USAGE

The following personal data is processed in connection with registration, based on consent (Art. 31 para. 1 DSG; Art. 34 para. 4 lit. b DSG; Art. 6 para. 1 lit a GDPR):

- › Technical identification number
- › Insurance number
- › Date of birth
- › Email address
- › Mobile phone number
- › Postcode
- › IP address

Other data that is collected:

- › Hash value of the password
- › Accepted version of the T&Cs
- › Compassana consent
- › Authentication information
- › FIDO device information

7.4 LOGS AND ANALYSIS

Activity of the User and of the business administrators in connection with online access is logged. In addition, analysis is carried out in anonymised form (such as the number of registered users).

7.5 DISCLOSURE TO THIRD PARTIES

Certain data processing activities are carried out by SWICA's contractual partner (in accordance with Art. 9 para. 1 DSG; Art. 6 para.1 lit. b GDPR). SWICA's contractual partner is contractually obliged to process data lawfully and to maintain confidentiality.

SWICA may share personal data if this is necessary to comply with the applicable laws and regulations, in connection with judicial proceedings or if required to do so by order of a court or government authority.

7.6 RETENTION

Upon termination of the Service, all User data relating to registration that is held by SWICA will be deleted to the extent that this is technically and reasonably possible and legally permissible. Data stored in backups is not subsequently removed.

7.7 DATA SECURITY

SWICA implements appropriate technical and organisational security precautions to protect personal data against unauthorised access and misuse (in accordance with Art. 3 DSG; Art. 25 GDPR).

7.8 RIGHTS OF DATA SUBJECTS

Under DSG and/or GDPR, data subjects have the following rights, so far as the relevant statutory conditions are met and there are no grounds on which to limit or defer such rights:

- › The right to ask SWICA whether and which data is processed
- › The right to request that any incorrect data be corrected
- › The right to request the erasure of data
- › The right to request that we provide certain personal data in a commonly used electronic format or that we transmit it to another controller
- › The right to revoke consent with future effect so far as the processing by SWICA is based on consent
- › The right to request and receive further information that is necessary for the exercise of these rights

If a data subject wishes to exercise the aforementioned rights, they must contact the controller as defined in section 7.1. In order for SWICA to exclude any misuse, an identity check must be carried out (for example with a copy of an official ID document such as an ID card or passport, whereby the information not required can be redacted). SWICA's data privacy notice contains further information on how data is processed:

- › [Data privacy notice Switzerland](#)
- › [Data privacy notice Liechtenstein](#)

VIII. FOREIGN LEGAL SYSTEMS IMPORT AND EXPORT RESTRICTIONS

Under some circumstances the use of Services abroad may violate the rules of foreign law. It is the User's responsibility to find out what rules apply. SWICA rejects all liability in this regard.

The User further acknowledges that there may be import and export restrictions for encryption algorithms which may be infringed if Services are used abroad.

IX. INTELLECTUAL PROPERTY

All intellectual property rights to the contents of the online access remain with the owners of these rights. Any reproduction, publication, modification or distribution of the contents of the online access without prior authorisation from SWICA is prohibited.

X. WARRANTY AND LIABILITY

SWICA takes all appropriate technical and organisational measures to ensure the proper operation of the Services, but cannot guarantee that the Services will be available at all times or will be error-free. In particular, maintenance work may cause temporary interruptions to the Services. If the User suffers any loss or damage in these cases, SWICA will not be held liable.

To the extent possible under the law, SWICA rejects all liability for direct or indirect loss or damage which the User may suffer in connection with using the Services. In particular, this includes loss or damage caused as a result of using information or by transmission errors, technical problems, interruptions, disruptions or illegal acts by third parties.

Nor will SWICA be held liable if the Services are interrupted, limited in part or in whole, or rendered inoperative due to force majeure or third-party culpability. Force majeure includes but is not restricted to power failure, malware (e.g. viruses), natural phenomena of special intensity (e.g. earthquakes, avalanches, floods and landslides), war-like events, insurrection and unforeseeable official restrictions.

XI. FEES AND CHARGES

The establishment of online access is free to the User. SWICA reserves the right to introduce charges or amend existing charges at any time. In such cases, new General Terms and Conditions will be submitted to Users for acceptance in accordance with section 2.2.

XII. APPLICABLE LAW AND PLACE OF JURISDICTION

All legal relationships of the User are subject to Swiss law, excluding any conflict-of-law rules and the provisions of the UN Convention on Contracts for the International Sale of Goods (CISG). The exclusive place of jurisdiction is SWICA's head office in Winterthur, unless otherwise provided for in mandatory Swiss law or the General Insurance Conditions (GIC) for insurance contracts.

XIII. FINAL PROVISIONS

If any provision of these General Terms and Conditions should be or become ineffective, this will not affect the effectiveness of the remaining provisions.

All ancillary arrangements and agreements between the User and SWICA must be in writing. The place of performance is SWICA's head office.

Version 7.0/2024