A + A Assureurs Associés SA
Research, investment and management of insurance portfolios
Place St-Gervais 1 I CP 1213 I CH-1211 Geneva 1
t +41 22 716 19 19 I f +41 22 731 85 21
info@synerisk.ch I www.synerisk.ch

Internal data protection guidelines for A + A Assureurs Associés SA

A. Foreword

A + A Assureurs Associés SA (hereinafter also referred to as the "employer"), it is important to process personal data in accordance with the law.

Management is responsible for the lawful processing of personal data, applies these guidelines itself and ensures that employees process data in compliance with them.

Sébastien Beck has been appointed Internal Data Protection Officer and acts as the internal contact person for data protection queries.

Sébastien Beck
Sebastien.beck@synerisk.ch
Phone +41 22 716 19 19

B. Data protection

1. What is personal data?

All information that makes it possible to identify a specific natural person is personal data (for example, name, address, date of birth, IBAN number, police number, social security number, health-related data, criminal sanctions, but also, in certain circumstances, the device ID and other device identification data).

2. What is personal data processing?

Any handling of personal data, in particular the collection, recording, storage, use, modification, communication, archiving, deletion or destruction of data, constitutes processing of personal data.

3. When is the processing of personal data by employees authorised?

Personal data may only be processed by employees in connection with the performance of their contractual obligations. Any other processing of data by employees is prohibited.

Employees' system authorisations are defined on the basis of their functions and implemented by technical and organisational measures. Authorisations for individual employees can be restricted or extended at any time.

4. How is personal data stored and protected?

The employer takes technical and organisational measures to protect data. Data is thus protected against destruction, unauthorised access, unlawful processing and loss. The measures taken are checked at least once a year and adapted if necessary.

Once the purpose of processing has been achieved, personal data is destroyed or rendered anonymous in accordance with internal deletion guidelines. The person responsible for physical destruction is Sébastien Beck, Director, and the person responsible for electronic destruction is Sébastien Beck, Director.

Data that must be kept for longer due to legal or other retention obligations is excluded from deletion.

Commercial documents must be kept for 10 years in accordance with Art. 958f para. 1 of the Swiss Code of Obligations. General tax documents must be kept for 10 years in accordance with art. 70 para. 2 of the Value Added Tax Act. Art. 42 para. 6 of the Value Added Tax Act must be kept for 10 years. Documents used as evidence or required for other objective reasons must be kept for longer.

5. What personal data is processed?

Employees should only collect and process personal data that is necessary to achieve their objectives (data minimisation).

Some data processing operations, such as archiving, are necessary for the employer to fulfil its legal or contractual obligations.

6. What other factors should employees take into account when processing personal data?

If a mandate exists with a client company, direct contact with the client's employees is only authorised if it is necessary for the execution of the insurance contract or the clarification of the claim.

If employees of the client company are contacted directly for other purposes, for example to negotiate other insurance policies, it must be ensured that these people have given their consent to being contacted.

7. How do employees deal with requests from the people concerned?

Under the new Swiss Data Protection Act, data subjects may request that their personal data be provided, transmitted, corrected or deleted. They may also object to unlawful processing or revoke their consent (e.g. opt-in for a newsletter).

All letters, telephone calls, e-mails or other correspondence containing such requests will be

forwarded immediately to Sébastien Beck, Administrator. He is responsible for coordinating and responding to requests. No requests will be answered by telephone.

Requests will only be accepted if the person concerned has provided appropriate proof of identity and if there are no legal grounds for deferral, restriction or exclusion.

In principle, there is no charge for responding to requests. For particularly voluminous requests, a contribution to costs of up to CHF 300 may be requested.

8. What do employees have to declare?

An IT security incident can occur, for example, when an employee clicks on a URL in a suspicious e-mail, opens a suspicious attachment, executes macros in documents, when data is encrypted, when access data is lost or transmitted, or when personal data is communicated to unauthorised persons (for example, sending an e-mail to several recipients who do not know each other without using the Bcc function; communicating personal data by telephone without checking the identity of the caller).

Employees should immediately report any suspicion or knowledge of an IT security incident to Sébastien Beck, Administrator. The loss of equipment used for business purposes or physical documents must also be reported without delay.

If personal data is involved, the person responsible immediately refers the matter to management, who then decides on internal and external communication and any notification to the Federal Data Protection Commissioner and, where applicable, other supervisory authorities.

9. What sanctions can be imposed on employees?

All employees shall ensure that all data and information that comes to their knowledge in the course of their employment relationship is treated confidentially. If employees fail to comply with their duty of confidentiality, the employer and/or the person affected by the breach may call the employee to account.

Employees may be punished if they intentionally breach their obligations (breach of professional or business secrecy in accordance with art. 62 of the Swiss Data Protection Act or art. 162 of the Swiss Criminal Code).

C. Information security

10. How do employees use IT tools?

The employer provides employees with computers and other IT infrastructure to enable them to fulfil their contractual obligations. In order to guarantee data protection, employees must implement the following measures:

- All equipment, networks and software required to fulfil contractual obligations are made available to employees. Any other unauthorised infrastructure must not be used for business purposes.
- Private devices must not be used for business purposes and must not be connected to the employer's network devices.
- The basic settings of devices, networks or software must not be modified by employees.
- The network used for the remote office or home office (e.g. Handyhotsport) must be protected by a strong password. Public, non-password protected networks can only be used via a VPN.
- IT infrastructure support is provided by Sébastien Beck, Administrator.
- Employees should not install any additional software without consulting Sébastien Beck, Administrator.

11. How do employees protect their information?

11.1. Connection data

Careful use of login data is an important part of data security. Employees must comply with the following rules:

- Employees are required to choose unique and strong passwords. Passwords and user names used for professional purposes must not be used for private purposes and must not be made known to others.
- Passwords should only be used for specific access.
- No passwords should be written down. If the employer provides password solutions, the employee must use them.

11.2. Data storage

Business data may only be stored on file storage systems provided by the employer. No business data may be stored on private file storage systems or in the cloud. If email, calendar or other applications are synchronised on private devices, they must be excluded from any cloud backups.

11.3. Communication

Personal data and business information considered confidential must be communicated securely. Employees must therefore comply with the following instructions:

- If insurance companies provide portals for downloading information, these must be used by employees.
- If sensitive personal data or confidential information is sent by e-mail, the e-mails are encrypted from end to end or the transmission takes place via an encrypted link or a secure platform.
- If secure transmission is not possible, the customer will be asked to confirm in writing that he/she accepts ordinary data transmission (e.g. as an e-mail attachment).
- If sensitive or confidential information, in particular passwords, are sent by post, the documents are sent by registered mail/courrier plus.
- Employees telephoning outside the workplace must ensure that no unauthorised third party is privy to personal data or business secrets.
- During video calls, no uninvolved third party may be visible in the camera field. Recordings are only authorised if they have been announced in advance.
- When sharing their screen, employees must ensure that unauthorised third parties do not have access to professional data.
- Private messaging services must not be used for professional communications.

11.4. Clean Desk and Clear Screen policy

Employees follow a Clean Desk and Clear Screen policy and undertake to comply with the following instructions:

- They put away all documents and files at the end of the day or in the event of prolonged absence.
- After meetings, all documents and files are removed from the meeting room. Information on whiteboards and flipcharts is also removed or destroyed.
- When employees leave their workstations, they lock all screens or log off. This also applies to short absences such as coffee breaks.

11.5. Access and entry restrictions

Employees must not allow unauthorised third parties access to non-public premises. External persons may not enter premises not accessible to the public unaccompanied.

11.6. How is protection against malware ensured?

Malicious software represents a high risk to data security. Employees are therefore required to observe the following instructions:

- Employees must not disable or bypass installed software.
- Employees must install all official updates and upgrades without delay.
- Attachments and documents from unknown senders should not be opened. Employees should report suspicious e-mails to Sébastien Beck, Administrator.
- Links to external websites should only be clicked if they are secure.
- No documents or software should be downloaded from unknown websites.
- Wherever possible, employees should only visit SSL-certified websites.

- No private e-mail should be forwarded to business e-mail addresses.

11.7. What guidelines should employees follow when using the Internet?

Using the Internet can pose a risk to data security. Employees must therefore comply with the following rules:

- Browsing the Internet and downloading documents are authorised for professional purposes only.
- It is forbidden to visit websites whose content includes: pornographic, sexist, racist or violence-promoting statements or representations; pyramid and snowball systems; the promotion and financing of terrorism; online casinos; or any other content that is illegal or contrary to accepted standards of behaviour.
- Commercial information must not be downloaded from the Internet, and in particular no content must be entered into free translation tools or chatbots or other artificial intelligence applications. These tools may re-use the information entered to train their artificial intelligence models and systems.

D. Contact

Questions or comments may be sent to the following address:

Sébastien Beck
Sebastien.beck@synerisk.ch
Phone +41 22 716 19 19

E. Effect

This directive comes into force on 01.01.2024.