Brief report

Audit
Audited data protection insurance products "Health

Allianz SE | Group Privacy
Königinstr. 28
80802 Munich

25.11.2022

Table of contents

1 Management summary

1.1 Tabular summary

Category	Chapter	Determination	

1.2 Final evaluation

All essential requirements of the current criteria catalog were met. Detailed test results

can be found in chapter 4 "Test results".

Bonn, the 25.11.2022

tekit Consult Bonn GmbH
TÜV Saarland Group

2 Project description

ClientAllianz SE | Group
Privacy Königinstr. 28
80802 Munich

Contractortekit Consult
Bonn GmbH TÜV
Saarland Group
Alexanderstr. 10
53111 Bonn

Test Report	TR45020
Project number	P45020
	Requirements CatalogTested Data Protection TEK0100SY Version 5.0
	Subject of the auditThe insurance products for private customers (Health & Leisure) of Allianz Private Krankenversicherungs-AG offered at www.allianz.de.
On-site	auditOn 20.07.2022, an on-site appointment took place at the client's premises.
Other audit comment	

3 Evaluation scheme

Category	Meaning/Consequence	
Note	The standard requirement or otherwise specified requirement is fully met. However, there is potential for improvement.	
Deviation	Deviation from a standard requirement or otherwise specified requirement that is not expected to have a direct effect on the outcome of the conformity assessment and that does not call into question the basic effectiveness of the system.	
Critical deviation	Deviation from a standard requirement or otherwise specified requirement that is expected to have a direct impact on the outcome of the conformity assessment, calls into question the fundamental effectiveness of the system, or the repeated occurrence of a deviation to the same (standard) requirement.	

4 Test results

The test results are described below. This evaluation is an excerpt of the overall findings. It has been compiled on the basis of the currently valid catalog of requirements and serves as basic information for the concluding audit comment.

4.1 Basic requirements for data protection organization

If the company falls within the scope of the GDPR, a data protection organization must be established.

4.1.1 Applicability of the GDPR

The General Data Protection Regulation applies if the controller has its registered office within the European Union or offers its goods and services there in accordance with the place of market principle.

The provisions of the GDPR must be observed, as its scope of application is opened.

4.1.2 Processing principles

The GDPR establishes the principle of "prohibition with reservation of permission". The processing of personal data is only permissible if there is an element of permission.

5 indications were found with regard to data protection statements and consents of the data subjects. In addition, one deviation from the standard requirement regarding data subjects' consents was identified, which is not expected to have a direct impact on the outcome of the conformity assessment and does not call into question the basic effectiveness of the system.

4.1.3 Data protection management

The company must demonstrate compliance with data protection requirements (accountability).

The standard requirement or otherwise specified requirement relating to data protection - management is fully met.

4.2 Data Protection Officer

Under certain conditions, the company is obliged to appoint a data protection officer.

4.2.1 Appointment of a company data protection officer

If required, a data protection officer must be appointed in writing and must have the necessary expertise and reliability to perform his or her duties. The data protection officer must report directly to the management and must not be subject to directives in the performance of his/her duties.

The standard requirement or otherwise specified requirement relating to the appointment of the data protection officer is fully met.

4.2.2 Tasks of the data protection officer

The data protection officer must fulfill the tasks specified by law. His tasks include, above all, monitoring that the employees involved in the processing operations are sensitized and trained (cf. Art. 3r (1) (b) GDPR).

The standard requirement or otherwise specified requirement relating to the tasks of the data protection officer is fully met.

4.2.3 Data transfer to third countries

Insofar as a cross-border transfer of personal data takes place, the special requirements of the GDPR must be taken into account. If personal data is transferred to insecure third countries, the company shall demonstrate an adequate level of data protection.

The standard requirement or otherwise specified requirement is fully met. A note was identified with regard to the documentation on data transfer to third countries.

4.2.4 Directory of processing activities

Each controller or processor shall keep a register of all processing activities under its responsibility (Art. 30 GDPR). It represents the starting point for the definition and knowledge of existing data processing operations in the company. It thus forms the basis for detailed accountability for compliance with data protection law.

A deviation from the standard requirement has been identified with regard to possible in-house processing on behalf of the company, which is not expected to have a direct impact on the result of the conformity assessment and which does not call into question the basic effectiveness of the system.

4.2.5 Data Breach Notification

In the event of a high-risk personal data breach, the service provider shall establish an effective process for notification to the competent supervisory authority.

The standard requirement or otherwise specified requirement related to data breach reporting is fully met.

4.2.6 Data protection impact assessment

In order to ensure compliance with this Regulation also in cases where the processing operations are likely to result in a high risk to the rights and freedoms of natural persons, the controller shall carry out a data protection impact assessment in advance, to assess the consequences for the protection of personal data and to be able to take the results of this assessment into account when choosing appropriate measures (Art. 35 GDPR).

The standard requirement or otherwise specified requirement related to privacy impact assessments is fully met.

4.2.7 Stakeholder inquiries

The GDPR protects data subjects and therefore provides for rights of data subjects that give rise to a claim against the company. The company should therefore establish processes to be able to respond to requests without delay.

One note was identified in relation to the privacy notices. In addition, one deviation from the standard requirement was identified in relation to cookie banners, which is not expected to have any direct impact on the outcome of the conformity assessment and does not call into question the basic effectiveness of the system.

4.3 Proceedings of the supervisory authorities as well as judicial and other proceedings

Requests, exchange of information, audits, sanctions and procedures based on data protection control mechanisms

4.3.1 Measures taken by data protection supervisory authorities

The company must provide all correspondence with data protection supervisory authorities from the last 24 months. These documents must not show that the effectiveness of the company's data protection processes is impaired in whole or in part.

The standard requirement or otherwise specified requirement regarding data protection supervisory authority measures is fully met.

4.3.2 Proceedings following actions by supervisory authorities, including judicial and other proceedings

The Company must provide all correspondence relating to completed, threatened, initiated, ongoing legal actions, administrative or civil proceedings, administrative or criminal sanctions, or other proceedings arising from the processing of personal data during the previous 24 months. These documents must not show that the effectiveness of the Company's data protection processes is impaired in whole or in part.

According to the client, there were no procedures for this test point.

4.4 Other data protection topics

Public and non-public entities that process personal data are obliged to ensure the execution of the GDPR as well as other regulations on data protection in this work.

4.4.1 Deletion concept

The GDPR stipulates that personal data must be deleted, for example, when the purpose of the processing no longer applies. In contrast, there are different legal/contractual retention periods for different documents. For this reason, the company should have created a deletion concept that categorizes the different personal data in more detail and defines deletion routines and retention periods that depend on this.

The standard requirement or otherwise specified requirement is fully met. A note was found with regard to the documentation of the extinguishing concept.

4.4.2 Confidentiality obligations of employees

Personal data may only be processed in a manner that includes appropriate security, including protection against unauthorized or unlawful processing.

The standard requirement or otherwise specified requirement regarding employee confidentiality obligations is fully met.

4.4.3 Employee data protection

Personal data of employees may be processed for purposes of the employment relationship if this is necessary for the decision on the establishment, implementation or termination.

The standard requirement or otherwise specified requirement relating to employee data protection is fully met.

4.5 Use of service providers

When using service providers, the company should assess the permissibility under data protection law and comply with the relevant requirements.

4.5.1 Job processing

To the extent that the Company discloses personal data to a processor, it shall do so only if the processor provides sufficient guarantees that appropriate technical and organizational measures will be implemented in such a way that the processing will be carried out in compliance with the requirements of this Regulation and will ensure the protection of the rights of the data subject.

The standard requirement or otherwise specified requirement is fully met. Two indications were identified in relation to processing operations.

4.5.2 Other service providers

Insofar as the company passes on personal data to other service providers, technical and organizational measures shall be taken to ensure that the risk to the rights of the data subjects is limited.

The standard requirement or otherwise specified requirement is fully met. A note has been identified regarding the use of other service providers.

4.6 Technical and organizational measures

After the adequacy check has been carried out, the company must implement suitable technical and organizational measures that enable personal data to be processed in compliance with the law and provide evidence of this.

4.6.1 Ensuring confidentiality

The technical and organizational measures are intended to ensure that data is protected against unauthorized access or disclosure.

The standard requirement or otherwise specified requirement related to ensuring confidentiality is fully met.

4.6.2 Ensuring integrity

The technical and organizational measures are intended to ensure that data is protected against unauthorized modification.

The standard requirement or otherwise specified requirement related to ensuring the integrity of data is fully met.

4.6.3 Ensuring availability and resilience

The technical and organizational measures are intended to ensure that data can be used when required and is not withheld without authorization.

The standard requirement or otherwise specified requirement with respect to ensuring the availability and resilience of data is fully met.

4.7 Requirements for secure data transmissions

The operator must ensure that the data transmission is encrypted according to the state of the art.

4.7.1 Protocols used

The SSL/TLS encryption protocols used must be state of the art.

The standard requirement or otherwise specified requirement regarding the protocols used is fully met.

4.7.2 Cipher Suites Offered

Cipher suites must be state of the art.

The standard requirement or otherwise specified requirement relating to the Cipher Suites provided is fully met.

4.7.3 Certification Authority

The certificates used must be traceable to a trusted certification authority.

The standard requirement or otherwise specified requirement relating to the certificates used is fully met.

4.7.4 Session management

Appropriate measures are taken to ensure that active sessions are secured in accordance with the state of the art.

The standard requirement or otherwise specified requirement is met. Only a hint regarding the use of the security header settings was found.

4.8 IT infrastructure

Sensitive data must be adequately protected by effective structural, technical and organizational measures. These include secure authentication mechanisms, encryption of data transmission channels in accordance with the state of the art, and appropriate protection of the connected server infrastructures in accordance with current security standards. Precautions must be taken with regard to effective system monitoring and regular maintenance cycles must be observed.

4.8.1 Passwords

If the system uses user accounts, state-of-the-art password policies must be followed. The user must be provided with suitable and secure procedures for changing passwords and for requesting forgotten passwords.

The standard requirement or otherwise specified requirement regarding the authentication mechanisms used is fully met.

4.8.2 Tracking services

The use of tracking services is only permitted with the (prior) consent of the data subject. If tracking, analysis and statistics services are used that collect, process or use personal data, the operator must include appropriate information in the privacy notices and separately obtain consent to use these services.

Two deviations from the standard requirement regarding cookie settings and privacy information were identified, which are not expected to have an immediate impact on the outcome of the conformity assessment and do not call into question the basic effectiveness of the system.

4.8.3 Monitoring

The operator must take appropriate measures to monitor the system.

The standard requirement or otherwise specified requirement related to the implemented monitoring measures is fully met.

4.8.4 System maintenance

The IT infrastructure must be regularly maintained and updated. The operator must define and have effectively implemented a process to identify and immediately address critical vulnerabilities.

The standard requirement or otherwise specified requirement related to system maintenance is fully met.

4.8.5 Firewall

A suitable firewall must be in place and actively managed.

The standard requirement or otherwise specified requirement regarding the implemented use of firewalls is fully met.

4.8.6 Virus protection

The operator must ensure that appropriate virus protection is in place and regularly updated.

One deviation from the standard requirement with regard to the documentation of the virus protection concept was identified, which is not expected to have a direct impact on the result of the conformity assessment and which does not call into question the basic effectiveness of the system.

4.8.7 Network protection

Suitable measures must be taken for network protection. Fail-safe operation of critical components must be ensured.

The standard requirement or otherwise specified requirement related to network protection is fully met.

4.8.8 Rights and roles

A rights and roles concept must be implemented and regularly reviewed.

One deviation from the standard requirement with regard to the documentation of the rights and roles concept was identified, which is not expected to have a direct impact on the result of the conformity assessment and which does not call into question the basic effectiveness of the system.

4.8.9 Backup and restore

An effective back-up and restore concept must be ensured. In particular, effective recovery of systems/data must be ensured in the event of a system failure.

The standard requirement or otherwise specified requirement with regard to the use of the implemented backup concept is completely fulfilled.

4.8.10 Data center

The data center must be state of the art and sufficiently physically secured.

The standard requirement or otherwise specified requirement is fully met.

4.8.11 Storage of data with high protection requirements

Data with a high protection requirement is encrypted using state-of-the-art methods.

The standard requirement or otherwise specified requirement relating to the storage of data with high protection needs is fully met.

4.8.12 Protection against current threats

The operator responds promptly to current security threats.

The standard requirement or otherwise specified requirement related to protection against current security threats is fully met.

4.9 Development, test, release process

To ensure the quality of the system, the operator shall ensure, by means of appropriate procedures, that an adequate standard is maintained in the development of the product.

4.9.1 Basics of the development process

Development and documentation follow regulated processes. The operator takes appropriate measures to ensure that processes and guidelines are adhered to.

The standard requirement or otherwise specified requirement related to the development process is fully met.

4.9.2 Requirements management

The requirements of new developments or significant changes to the test item must be defined in writing. A release process must be demonstrated.

The standard requirement or otherwise specified requirement related to requirements management is fully met.

4.9.3 Test and release procedure

The operator must operate adequate quality assurance and meet selected minimum requirements. A process for testing and releasing new functions and developments must be defined and effectively implemented.

The standard requirement or otherwise specified requirement relating to the test and release procedure is fully met.

5 Disclaimer

The assessment was carried out to the best of our knowledge and belief, with the necessary care and exclusively on the basis of the publicly available information of the regulations at the time of the assessment. Furthermore, all findings from this assessment refer only to the random samples that were taken during the course of the assessment. It is possible that further findings could be made in the course of additional samples. Therefore, no claim to a fully comprehensive evaluation can be derived from the assessment report, nor can an evaluation of future certifications and approvals be derived.