Technical and organisational measures of the SoSci Survey GmbH

Revision from 04/19/2020

General Information

As an organizational background to the technical and organizational measures of SoSci Survey GmbH (processor), the following information should be mentioned beforehand:

Personal data is in general processed on the technical equipment of a subcontractor (webhoster). The technical equipment (web server) of the subcontractor is located in a computer center certified according to ISO27001. For this housing, the webhoster uses the services of another company (operator of the computer center), which is not a subcontractor in the sense of the GDPR.

A large part of the technical measures to protect the processed data (in particular the physical access to the systems) therefore results from the technical and organizational measures (TOM) of the computer centre, which are available to the processor and can be viewed upon request.

- When using the survey server **s2survey.net**, no processing usually takes place on the processor's equipment.
- The use of the survey server **www.soscisurvey.de** is not covered by this document.

Any transfer or other processing of the data to the processor's system(s) beyond the normal case will only take place on written instructions from the responsible party (controller), for example in order to clarify inconclusive technical or content issues. The technical and organisational measures employed in this case are set out in the following description.

1. Confidentiality

1.1. Access Control Rooms

Survey Server

Regarding the server rooms, we refer to the technical and organizational measures (TOM) of the webhoster (quoted below) and the computer center:

All computer rooms are equipped as separate IT security rooms in the sense of the IT basic protection catalogue, published by the German Federal Office for Information Security (BSI), according to the requirements of the category "basic protection".

The data security rooms offer protection against the following risks:

- Fire according to DIN 4102-2 / F90, with approval by the construction supervisory authority
- Temperature limits and humidity for 30 minutes according to EN 1047-2
- Smoke protection according to DIN 18095
- unauthorised access / burglar resistance WK II according to EN 1627
- Fire-fighting water inlet with watertightness certificate according to EN 60529 / IP 56
- Dust tightness according to EN 60529
- Protection against sabotage / vandalism
- EMC protection
- Protection against increased debris loads

1.2. Access Control Data

All data processing systems (both local and the survey servers used) are secured by passwords. At least the following standards are complied with:

Minimum standards for passwords	• Different characters composition • Minimum length 10 characters • Access blocking after more than 3 login attempts
Password management	• Established open source software • Access protection by means of 2-factor authentication

Survey Server

Access controls based on software and configuration:

Software used on the server	• Common Linux distribution (open source) • Common web server applications (open source)
Restriction of server access	• Restriction to necessary ports (HTTP, HTTPS, e-mail) by means of internal firewall (iptables) • The SSH management port is only accessible for selected IP addresses.
Security updates	• Security updates are installed automatically several times a day.

With regard to the physical access controls to the web server, we again refer to the TOM of the web hoster, quoted below:

Only authorized persons have access to the data processing equipment with which personal data are processed or used.

Determination of authorized persons	• Rooms are locked and only authorized persons have a key • Access monitoring in the computer center • Biometric security systems for office and computer centre areas • Chip card/transponder for security areas
Rules for noncompany members	• External persons have no access to the data processing equipment
Protection outside working hours	• All rooms are locked • Camera surveillance
Workstations and notebooks	• Notebooks are encrypted • Authentication via user name/password • Internal security guideline for the handling of data processing systems
Obligation of data secrecy	• Performed for each employee
User permissions	• Are assigned by the IT manager
Use of 2-Factor	• Where possible, a 2-factor authentication is used

Destruction of data media	• Is carried out by a certified company • Destruction is documented.
Remote access	• The administrative remote access to the data processing systems is only possible via a VPN
IT Security	• Use of various antivirus solutions • Use of hardware and software firewalls

Administrative systems

Personal data is stored on an external/mobile medium exclusively for the purpose of storing the backups described above. Encryption according to the PGP standard is used (key length min. 2048 bit).

Anti-virus software is used on the processor's data processing systems, security updates are installed automatically, the Internet connection is established via NAT router.

1.3. Access Control

Since only the managing directors have access to personal data, SoSci Survey GmbH does without a detailed role concept.
The processing of the data is automated, there is no regular access to the processed data by employees or management. Such access only takes place if the controller requests it in writing, for example to clarify specific facts. In general, all systems use time locks:

- Auto-Logout/Screen lock
- Locking after invalid login attempts
- Delayed response behaviour in case of failed attempts

1.4. Pseudonymisation

Pseudonymisation of Survey Data

In case the mailing feature of SoSci Survey is used and the data protection mode for the addressees is set to another mode than "anonymous", a reference between collected data and address entry is stored in the database. Unless the data protection mode "person-related" has been selected for the address entries, this reference is not visible to the controller – from the point of view of the controller, effective pseudonymisation is provided.

Anonymization of Survey Data

The software feature "Collect Email Addresses Separately" allows an e-mail address or other personal data (address entries) to be queried and stored separately within a questionnaire. The storage takes place in such a way that (as soon as there are at least two data sets or at least two contact entries) it is no longer possible to relate individual address entries to individual data sets of the survey.

1.5. Separation Control

SoSci Survey is a multi-client system that basically separates both entered and collected data within a relational database according to survey projects (internal multi-client capability, internal allocation).

The backup of the data includes the entire survey server (no differentiation between survey project/client), address data which allow for personal reference within the serial mail function are backed up separately.

Test-/development system and productive system (survey server) run on different hardware in different networks, the test system has no access to the data of the productive system.

2.Integrity

2.1. Control of transfers

All data transports are conducted via network transmission (encrypted data transmission), data carriers are not used. Data is transferred by using the following modes:

Access to the Web Interface

The transmission of input and collected data between the processor and the survey server is protected by SSL encryption. On the s2survey.net server a certificate with extended validation is used for this purpose.

Participation in Surveys

Access to the questionnaire and the return transmission of the respondent's answers to the survey server is protected by SSL encryption. On the server s2survey.net a certificate with extended validation is used for this purpose.

Management access to the Survey Server

The administration of the survey server as well as possible access to the database is encrypted via SSH (data access via SSH tunnel).

Remote maintenance, if necessary, is carried out exclusively by the hosting subcontractor.

Hardware-based Measures

For the physical transfer control measures, reference is made to the TOM of the web hoster, cited below:

Determination of authorized persons	• Through the allocation of appropriate rights
Data carriers	• Mobile data carriers are not used in general. Storage takes place on permanently mounted hard disks • Hard disks are monitored and locked in the server racks
Selection of contractors	• Selection is usually made by the Head of IT or GF
Distribution of rights and obligations between contractor (controller) and client (processor)	• Accomplished through an data processing agreement (DPA) under Article 28 GDPR
Control of contractors	• Done by the Head of IT and the Data Protection Officer

2.2. Input control

Survey data is usually entered by the persons themselves, the time of when the data is entered is part of the collected data (time stamp, survey duration). Additional logging for individual survey projects can be optionally activated in the software.

Since the survey protocols are part of the data set, the controller is responsible for keeping them. The deletion of the collected data on the survey server is accompanied by a deletion of the meta-information on the survey.

3. Availability and Resilience

Availability Control

The services are provided with the help of a data center service provider that is certified according to ISO 27001. For detailed information, please refer to the TOM of m-net GmbH.

A disaster recovery backup is kept physically and locally separated.

An additional daily encrypted backup to restore accidentally deleted partial data is stored for a period of 1 month (s2survey.net) on a separate system in the same data center and is deleted automatically.

4. Regular Review, Assessment and Evaluation of the Effectiveness of Internal Data Protection

4.1. Incident Response Management

The technical operation of the survey servers is outsourced to a subcontractor (hoster). For the emergency concept and contingency plan for IT failure, reference is made to its TOM.

4.2. Order Control

Generally, personal data is automatically collected, processed, stored and transmitted to the controller by the survey software. These functions are accessed via the user interface.

Generally, there is no manual processing of the personal data that is processed on behalf of the controller, unless there is a written instruction from the controller.

Contractors (subcontractors) are selected by the management.

The division of rights and obligations between the contractor and the client is carried out by means of an data processing agreement (DPA) in accordance with Article 28 GDPR.

4.3. Data Protection Management

Data protection management is planned together with an external data protection officer with the involvement of the management. Data protection goals are defined and the need for action is determined and prioritized.