Technische und organisatorische Maßnahmen der SoSci Survey GmbH

Stand vom 01.12.2019

Rahmeninformation

Als organisatorischer Hintergrund zu den technischen und organisatorischen Maßnahmen der SoSci Survey GmbH (Verarbeiter) seien die folgenden Informationen vorangestellt:

Die Verarbeitung der personenbezogenen Daten erfolgt im Regelfall auf den technischen Anlagen eines Subunternehmers (Webhoster). Die technischen Anlagen (Webserver) des Subunternehmers sind in einem nach ISO27001 zertifizierten Rechenzentrum untergebracht. Für diese Unterbringung (Housing) greift der Webhoster auf die Leistungen eines weiteren Unternehmens (Betreiber des Rechenzentrums) zurück, welches allerdings kein Subunternehmer im Sinne der DSGVO ist.

Ein großer Teil der technischen Maßnahmen zum Schutz der verarbeiteten Daten (insbesondere der physische Zugriff auf die Anlagen) ergibt sich daher aus den technischen und organisatorischen Maßnahmen (TOM) des Rechenzentrums, welche dem Verarbeiter vorliegen und auf Anfrage eingesehen werden können.

- Bei Nutzung des Befragungsservers **s2survey.net** findet im Regelfall keine Verarbeitung auf den Anlagen des Verarbeiters statt.
- Die Nutzung des Befragungsservers **www.soscisurvey.de** ist nicht Gegenstand des vorliegenden Dokuments.

Eine über den Regelfall hinausgehende Übermittlung oder andere Verarbeitung der Daten auf die/den Anlagen des Verarbeiters findet nur auf schriftliche Weisung des Verantwortlichen hin statt, etwa um unschlüssige technische oder inhaltliche Sachverhalte zu klären. Die dabei ergriffenen technischen und organisatorischen Maßnahmen sind in der folgenden Darstellung enthalten.

1. Vertraulichkeit

1.1. Zutrittskontrolle

Befragungsserver

Hinsichtlich der Serverräume wird auf die technische und organisatorische Maßnahmen (TOM) des Webhosters (nachfolgend zitiert) und des Rechenzentrums verwiesen:

Alle Datenräume sind als separate IT Sicherheitsräume im Sinne des IT- Grundschutzkataloges, herausgegeben vom Bundesamt für Sicherheit in der Informationstechnik (BSI), gemäß Anforderung der Kategorie “Grundschutz“ ausgerüstet.

Die Datensicherheitsräume bieten Schutz vor folgenden Risiken:

- Feuer nach DIN 4102-2 / F90, mit bauaufsichtlicher Zulassung
- Temperaturgrenzwerte und Luftfeuchte für 30 Minuten gem. EN 1047-2
- Rauchschutz nach DIN 18095
- unbefugter Zutritt / Einbruchhemmung WK II nach EN 1627
- Löschwassereintritt mit Wasserdichtigkeitsnachweis gem. EN 60529 / IP 56
- Staubdichtigkeit gemäß EN 60529
- Schutz gegen Sabotage / Vandalismus
- EMV-Schutz
- Schutz gegen erhöhte Trümmerlasten

1.2. Zugangskontrolle

Sämtliche Datenverarbeitungssysteme (sowohl lokal wie auch die eingesetzten Befragungsserver) sind mittels Passwörtern gesichert. Dabei werden mindestens die folgenden Standards eingehalten:

Mindeststandards für Passwörter	• Unterschiedliche Zeichenzusammensetzung • Mindestlänge 10 Zeichen • Zugangssperre bei mehr als 3 Anmeldeversuchen
Verwaltung der Passwörter	• Etablierte Open Source Software • Schutz des Zugriffs durch 2-Faktor Authentifizierung

Befragungsserver

Auf Software und Konfiguration basierende Zugangskontrollen:

Verwendete Server-Software	• Gängige Linux-Distribution (Open Source) • Gängige Webserver-Anwendungen (Open Source)
Beschränkung von Server-Zugriffen	• Beschränkung auf notwendige Ports (HTTP, HTTPS, E-Mail) mittels interner Firewall (iptables) • Der SSH Verwaltungsport ist nur für ausgewählte IP-Adressen erreichbar.
Sicherheitsupdates	• Sicherheitsupdates werden automatisiert mehrmals täglich installiert.

Hinsichtlich der physischen Zutrittskontrollen zum Webserver wird erneut auf die TOM des Webhosters verwiesen, nachfolgend zitiert:

Nur befugte Personen haben Zugang zu den DV-Anlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden.

Festlegung befugter Personen	• Räume sind verschlossen und nur befugte Personen haben einen Schlüssel • Zutrittsüberwachung im RZ • Biometrische Sicherheitssysteme für die Büro- und RZ-Flächen • Chipkarten-/Transponder für Sicherheitsbereiche
Regelungen für Firmenfremde	• Betriebsfremde Personen haben keinen Zugang zu den DV-Anlagen
Sicherung außerhalb der Arbeitszeit	• Alle Räume sind verschlossen • Kameraüberwachung
Workstations und Notebooks	• Notebooks sind verschlüsselt • Authentifizierung über Benutzername/Passwort • Interne Sicherheitsrichtlinie für den Umgang mit DV-Systemen
Verpflichtung auf das Datengeheimnis	• Wird bei jedem Mitarbeiter durchgeführt
Benutzerberechtigungen	• Werden durch den Leiter IT vergeben
Einsatz von 2-Factor	• Wo es möglich ist, wird eine 2-Factor Authentifizierung verwendet

Vernichtung von Datenträgern	• Wird durch ein zertifiziertes Unternehmen durchgeführt • Die Vernichtung wird protokolliert
Remotezugriff	• Der administrative Remotezugriff auf die DV-Anlagen ist ausschließlich über ein VPN möglich
IT-Sicherheit	• Einsatz diverser Antivirenlösungen • Einsatz von Hard- und Softwarefirewalls

Verwaltungssysteme

Personenbezogene Daten werden ausschließlich zur Verwahrung der oben beschrieben Sicherheitskopien (Backups) auf einem externen/mobilen Medium gespeichert. Dabei kommt eine Verschlüsselung nach dem PGP-Standard zum Einsatz (Schlüssellänge min. 2048 Bit).

Auf den Datenverarbeitungsanlagen des Verarbeiters wird eine Anti-Viren-Software eingesetzt, Sicherheitsupdates werden automatisiert installiert, die Internetverbindung erfolgt nur mittels NAT-Router.

1.3. Zugriffskontrolle

Da nur die Geschäftsführer auf personenbezogene Daten zugreifen können, verzichtet die SoSci Survey GmbH auf ein detailliertes Rollenkonzept.

Die Verarbeitung der Daten erfolgt automatisiert, regelmäßig erfolgt kein Zugriff von Mitarbeitern oder Geschäftsführung auf die verarbeiteten Daten. Ein solcher Zugriff findet nur dann statt, wenn der Verantwortliche schriftlich darum bittet, etwa zur Klärung konkreter Sachverhalte.

Generell verwenden alle eingesetzten Systeme zeitlich Sperren:

- Auto-Logout/Bildschirmsperre
- Sperren nach ungültigen Anmeldeversuchen
- Zeitverzögertes Antwortverhalten bei Fehlversuchen

1.4. Pseudonymisierung

Pseudonymisierung von Befragungsdaten

Für den Fall, dass die Serienmail-Funktion von SoSci Survey verwendet und für die Adressaten ein anderer Datenschutz-Modus als „anonym“ eingestellt wurde, ist in der Datenbank ein Bezug zwischen erhobenen Daten und Adresseintrag hinterlegt. Sofern nicht der Datenschutz-Modus „personenbezogen“ für die Adresseinträge ausgewählt wurde, ist diese Zuordnung für den Verantwortlichen nicht einsehbar – aus Sicht des Verantwortlichen liegt eine effektive Pseudonymisierung vor.

Anonymisierung von Befragungsdaten

Die Software-Funktion „Kontaktdaten getrennt erheben“ erlaubt die Abfrage und getrennte Speicherung einer E-Mail-Adresse oder anderer personenbezogener Daten (Adresseinträge) innerhalb eines Fragebogens. Die Speicherung erfolgt derart, dass (ab dem Vorliegen von mindestens zwei Datensätzen oder mindestens zwei Kontakteinträgen) eine Zuordnung einzelner Adresseinträge zu einzelnen Datensätzen der Befragung nicht mehr möglich ist.

1.5. Trennungskontrolle

SoSci Survey ist ein Mehr-Mandantensystem, welches sowohl eingegebene als auch erhobene Daten innerhalb einer relationalen Datenbank grundsätzlich nach Befragungsprojekten trennt (interne Mandantenfähigkeit, interne Zweckbindung, Abschottung, Löschung).

Die Sicherung der Daten (Backup) erfolgt für den gesamten Befragungsserver (keine Differenzierung nach Befragungsprojekt/Mandant), Adressdaten welche im Rahmen der Serienmail-Funktion eine Personenbeziehbarkeit erlauben, werden getrennt gesichert.

Test-/Entwicklungs-System und Produktivsystem (Befragungsserver) laufen auf unterschiedlicher Hardware in unterschiedlichen Netzen, das Testsystem hat keinen Zugriff auf die Daten des Produktivsystems.

2.Integrität

2.1. Weitergabekontrolle

Alle Datentransporte erfolgen mittels Netzwerkübermittlung (verschlüsselte Datenübertragung), Datenträger kommen nicht zum Einsatz. Folgende Datentransporte finden Anwendung:

Zugriffe auf das Web-Interface

Die Übermittlung von Eingaben und erhobenen Daten zwischen dem Verarbeiter und dem Befragungsserver ist durch SSL-Verschlüsselung geschützt. Auf dem Server s2survey.net kommt dafür ein Zertifikat mit erweiterter Validierung (Extended Validation) zum Einsatz.

Teilnahme an Befragungen

Der Aufruf des Fragebogens und die Rückübermittlung von Daten des Befragten an den Befragungsserver ist durch SSL-Verschlüsselung geschützt. Auf dem Server s2survey.net kommt dafür ein Zertifikat mit erweiterter Validierung (Extended Validation) zum Einsatz.

Verwaltungszugriffe auf den Befragungsserver

Die Verwaltung des Befragungsservers sowie eventuelle Zugriffe auf die Datenbank erfolgen verschlüsselt mittels SSH (Datenzugriff via SSH-Tunnel).

Eine Fernwartung erfolgt, sofern erforderlich, ausschließlich durch den Hosting-Subunternehmer.

Hardware-basierte Maßnahmen

Für den Maßnahmen zur physischen Weitergabekontrolle wird auf die TOM des Webhosters verwiesen, nachfolgend zitiert:

Festlegung befugter Personen	• Durch die Vergabe entsprechender Rechte
Datenträger	• Mobile Datenträger werden in der Regel nicht verwendet. Speicherung findet auf fest montierten Festplatten statt • Festplatten werden überwacht und werden in den Server-Racks verschlossen
Auswahl der Auftragnehmer	• Auswahl erfolgt in der Regel durch Leiter IT oder GF
Aufteilung der Rechte und Pflichten zw. Auftragnehmer und Auftraggeber	• Geschieht über einen AV-Vertrag nach Artikel 28 DSGVO
Kontrolle der Auftragnehmer	• Geschieht durch den Leiter IT und den Datenschutzbeauftragten

2.2. Eingabekontrolle

Die Eingabe von Befragungsdaten erfolgt i.d.R. durch die Personen selbst, der Zeitpunkt der Dateneingabe ist Bestandteil der erhobenen Daten (Zeitstempel, Verweildauer). Eine zusätzliche Protokollierung für einzelne Befragungsprojekte kann optional in der Software aktiviert werden.

Da die Befragungsprotokolle Teil des Datensatzes sind, obliegt die Aufbewahrung dem Verantwortlichen. Die Löschung der erhobenen Daten auf dem Befragungsserver geht mit einer Löschung der Metainformationen zur Befragung einher.

3. Verfügbarkeit und Belastbarkeit

Verfügbarkeitskontrolle

Die Dienstleistungen werden mit Hilfe eines Rechenzentrumsdienstleisters erbracht, welcher nach ISO 27001 zertifiziert ist. Für detaillierte Informationen wird auf die TOM der m-net GmbH verwiesen.

Ein Desaster Recovery Backup wird physikalisch und örtlich getrennt aufbewahrt.

Ein zusätzliches tägliches, verschlüsseltes Backup zur Wiederherstellung versehentlich gelöschter Teildaten wird für den Zeitraum von 1 Monat (s2survey.net) auf einem getrennten System im gleichen Rechenzentrum gespeichert und automatisiert gelöscht.

4. Regelmäßige Überprüfung, Bewertung und Evaluierung der Wirksamkeit des internen Datenschutzes

4.1. Incident Response Management

Der technische Betrieb der Befragungsserver ist an einen Subunternehmer (Hoster) ausgelagert. Zum Havarie-Konzept und Notfallplan für IT-Ausfall wird auf dessen TOM verwiesen.

4.2. Auftragskontrolle

Im Regelfall werden die personenbezogenen Daten automatisiert durch die Befragungssoftware erhoben, verarbeitet, gespeichert und an den Verantwortlichen übermittelt. Diese Funktionen werden über die Benutzeroberfläche ausgelöst.

Im Regelfall erfolgt keinerlei manuelle Verarbeitung der personenbezogenen Daten, die im Auftrag verarbeitet werden, außer es liegt eine schriftliche Weisung des Auftraggebers vor.

Auftragnehmer (Subunternehmer) werden durch die Geschäftsführung ausgewählt.

Die Aufteilung der Rechte und Pflichten zwischen Auftragnehmer und Auftraggeber geschieht über einen AV-Vertrag nach Artikel 28 DSGVO.

4.3. Datenschutzmanagement

Die Planung des Datenschutzmanagements erfolgt gemeinsam mit einem externen Datenschutzbeauftragten unter Einbindung der Geschäftsführung. Dabei werden Datenschutzziele definiert und der Handlungsbedarf ermittelt und priorisiert.