

# Löschkonzept für den Befragungsserver s2survey.net

Stand vom 10.11.2018

Das nachfolgende Löschkonzept beschreibt die Speicherung und Löschung von personenbezogenen Daten, welche auf dem Befragungsserver *s2survey.net* im Rahmen von Befragungen mittels der Software SoSci Survey eingegeben und erhoben werden.

## 1. Beschreibung der Daten

Die Software *SoSci Survey* verarbeitet personenbezogene Daten in unterschiedlichen Teilprozessen. Es handelt sich dabei um folgend Daten:

1. *Angaben der Befragten* im Fragebogen, welche direkt im Datensatz gespeichert werden. Hierbei wird für jeden Befragten („Fall“) eine Datenzeile angelegt, welche durch eine fortlaufende Nummer („Fallnummer“) identifizierbar ist. In Sonderfällen (Multi-Level-Fragebögen) können für einen Befragten mehrere Fälle im Datensatz angelegt werden.
2. *Dateien*, welche von den Teilnehmern im Rahmen eines Interviews hochgeladen werden (Fragetyp „Datei hochladen“) oder durch Tonaufzeichnung (Fragetyp „Dateiinhalte übertragen“) entstehen.
3. *Kontaktdaten*, welche die Befragten im Fragebogen eintragen, die getrennt vom Datensatz und von anderen Adressdaten gespeichert werden (z.B. E-Mail-Adressen zur Teilnahme an einem Gewinnspiel, Fragetyp „Kontaktdaten getrennt erheben“).
4. *Adressdaten* zum Versand von Serienmails, welche entweder von der Projektleitung eingetragen oder vom Befragten durch eine Opt-In-Frage angegeben werden. Adressdaten können abhängig vom verwendeten Datenschutz-Modus mit Angaben der Befragten (1) verknüpft sein oder nicht.
5. *Daten zur Verwendung im Datensatz* (z.B. Zuspielen von Stammdaten), welche entweder von der Projektleitung eingetragen werden (Funktion „Datenbank für Inhalte“) oder im Rahmen von früheren Fragebögen im selben Befragungsprojekt erfasst wurden.

Darüber hinaus speichert die Software *Fragebögen und deren Inhalte* (z.B. Begrüßung oder Instruktionen), welche in aller Regel keine personenbezogenen Daten enthalten.

Die Daten eines Befragungsprojekts werden in virtuellen Datenbankpartitionen abgelegt, eine Trennung in einzelne Datenbanken erfolgt nicht. Hochgeladene/übermtragene Dateien werden in einem separaten Verzeichnis im Dateisystem gespeichert.

## 2. Manuelle Löschung

Die Löschung der oben beschriebenen Daten kann jederzeit manuell durch die Projektleitung selektiv oder gesamt erfolgen. Dafür stehen die folgenden Funktionen zur Verfügung:

- Befragungsprojekte können vollständig gelöscht werden, dies umfasst alle der oben genannten Teilprozesse sowie die Fragebögen und deren Inhalte.
- Befragungsprojekte können archiviert werden. Dabei werden der Fragebogen und dessen Inhalte in einer Datei gespeichert, anschließend werden alle Inhalt des Befragungsprojekts gelöscht.
- Die Angaben der Befragten (1) und die von Befragten hochgeladenen/übermittelten Dateien (2) können gemeinsam vollständig oder für einzelne Fälle gelöscht werden. Über die Funktion „Ausgefüllten Fragebogen ändern“ können einzelne Fälle geändert werden.
- Getrennt erhobene Kontaktdaten (3) können gesamt gelöscht werden.
- Adressdaten (4) können bearbeitet, einzeln oder gesamt gelöscht werden.
- Datei zur Verwendung im Datensatz (5) können einzeln oder gesamt gelöscht werden.

Bei der Löschung werden die Daten aus der Datenbank oder vom Datenträger gelöscht, es werden jedoch darüber hinaus für einen begrenzten Zeitraum Sicherheitskopien (Backups) aufbewahrt, die nachfolgende beschrieben.

### 3. Automatisierte Löschung

Falls keine manuelle Löschung erfolgt, wird ein Befragungsprojekt automatisch archiviert (Löschung aller Daten aus der Datenbank, Speicherung des Fragebogens und dessen Inhalte als Datei), wenn sich die Projektleitung 12 Monate lang nicht im Befragungsprojekt eingeloggt hat und in diesem Zeitraum auch keine neuen Daten erhoben wurden.

### 4. Sicherheitskopien

Gegen Datenverlust durch technische Fehler oder Bedienfehler werden regelmäßig Sicherheitskopien (Backups) erstellt. In diesen werden die oben genannten Daten auch über die Löschung hinaus zeitlich begrenzt gespeichert. Sicherheitskopien werden wie folgt erstellt:

- Ein tägliches Disaster Recovery wird einen Monat lang aufbewahrt.
- Eine tägliche Sicherheitskopie der Datenbank wird einen Monat lang aufbewahrt.
- Eine tägliche Sicherheitskopie des Dateisystems wird mindestens einen Monat und maximal zwei Monate lang aufbewahrt. Diese Sicherheitskopie betrifft hochgeladene/übermittelte Dateien, nicht aber die Datenbank.

Eine vorzeitige Löschung von Daten aus den Sicherheitskopien ist nicht möglich.

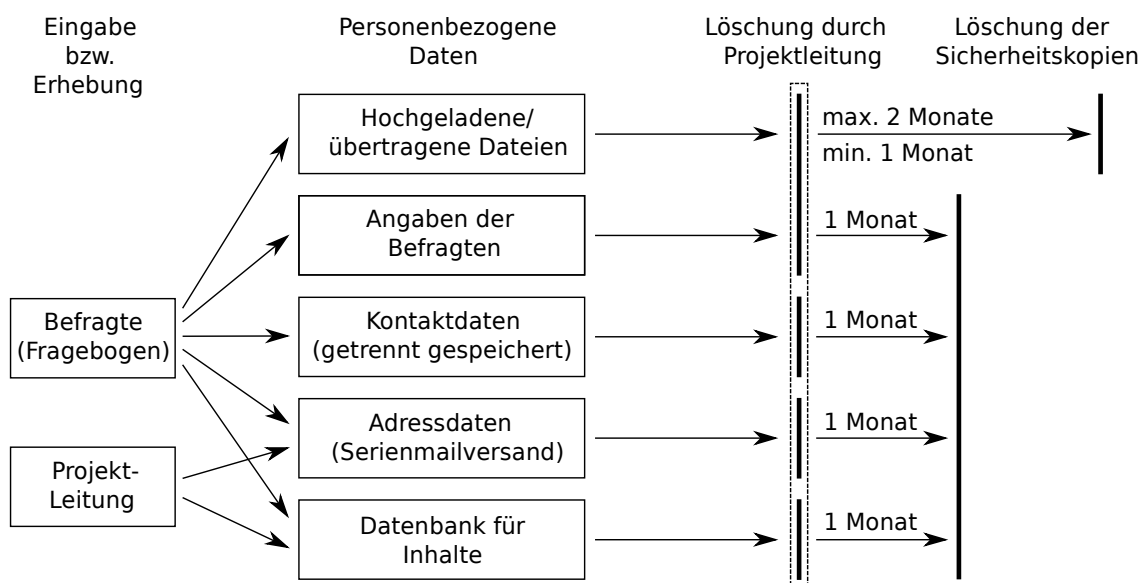


Abbildung 1: Speicherfristen personenbezogener Daten nach der Löschung in SoSci Survey

### 5. Dokumentation

Die Software dokumentiert bei der Löschung (manuell durch die Projektleitung oder automatisch nach Ablauf der Aufbewahrungsfrist) der folgenden Daten. Dabei wird der Zeitpunkt der Löschung, das Benutzerkonto, welches die Löschung veranlasst und die vom Anwender verwendete IP-Adresse dokumentiert:

- Angaben der Befragten (1) und hochgeladene/übermittelte Dateien (2), bei Löschung einzelner Fälle wird die Fall-Nummer (CASE) dokumentiert.
- Adressdaten (4), bei Löschung einzelner Einträge wird die Datenbank-ID und ein SHA1-Hash der E-Mail-Adresse bzw. Mobilnummer dokumentiert.

Die Dokumentation kann durch die Projektleitung jederzeit im Benutzerkonto heruntergeladen werden.

Die korrekte Funktion der Datensicherung und Löschung alter Sicherheitskopien wird von der eingesetzten Software automatisiert dokumentiert (Logfile).