«/Anlage §9 BDSG»

Massnahmenbeschrieb
zum Anlagenblatt §9 BDSG bei onlineumfragen.com GmbH

§9 BDSG

Öffentliche und nicht-öffentliche Stellen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften dieses Gesetzes, insbesondere die in der Anlage zu diesem Gesetz genannten Anforderungen, zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

Anlage (zu §9 Satz 1)

Werden personenbezogene Daten automatisiert verarbeitet oder genutzt, ist die innerbehördliche oder innerbetriebliche Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Dabei sind insbesondere Maßnahmen zu treffen, die je nach der Art der zu schützenden personenbezogenen Daten oder Datenkategorien geeignet sind,

1. Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, mittels angemessener Massnahmen zu verwehren (Zutrittskontrolle),

2. zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können (Zugangskontrolle),

3. zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (Zugriffskontrolle),

4. zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist (Weitergabekontrolle),

5. zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (Eingabekontrolle),

6. zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle),

7. zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle),

8. zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

Eine Maßnahme nach Satz 2 Nummer 2 bis 4 ist insbesondere die Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren.

Fassung aufgrund des Gesetzes zur Änderung datenschutzrechtlicher Vorschriften vom 14.8.2009 (BGBl. I S. 2814) m.W.v. 01.09.2009

Massnahmen bei onlineumfragen.com (Stand 1.1.2017)

1. Zutrittskontrolle

   Hochsicherheits-Rechenzentrum (Colozueri in Zürich sowie InterXion Zürich mit Bankenlizenz), raised floor, mit redundanten Klimaanlagen, Feuer- und Rauchmeldeanlagen (VESDA), Elektronische und physische Zutrittskontrollen in Server-Zentrum sowie Büro-Räumlichkeiten in Alpnach und Luzern (Serverräume mit Gesichtskontrolle, Schlüssel, PIN sowie Magnetkarte, Überwachungskameras, elektrische Türöffner, Serverräume und Büros mit Sicherheitstüren, Schlüssel zu Büroräumlichkeiten mit digitaler Ein-/Ausgangsüberwachung und Bildüberwachung, Schlüssel zu Rechenzentren nur bei autorisierten Mitgliedern der technischen Geschäftsleitung, welche die regelmässige Systemwartung und Serverpflege inhouse betreiben. Keine externen Servicepartner für Serverwartung). Backup-Medien in Bankschliessfach im Tresorraum einer Schweizer Bank. Serverräume mit redundanten Notstrom-Dieselgeneratoren und mehrfachredundanten Upstream-Provider (Carrier).

2. Zugangskontrolle

   Passwortvergabe/-schutz aller wesentlichen technischen Systeme, Protokollierung der Nutzung aller wesentlichen technischen Systeme und Prozesse, Log-Kontrollen durch die Geschäftsleitung

3. Zugriffskontrolle

   Alle Daten, welche von onlineumfragen.com verarbeitet werden, werden in einer redundanten, verteilten und replizierten Hochleistungsdatenbank des führenden Datenbankherstellers

gespeichert und mehrfach dezentral gesichert. Die Daten werden verschlüsselt gespeichert und sind durch zahlreiche technische Systeme geschützt. Wir verwenden für unsere Kunden ausschliesslich sichere, serverseitig vergebene, mindestens zehnstellige und sonderzeichenfähige Passwörter, welche auf leicht memorierbare Phoneme verzichten und bei internationalen Befragungen auf landesspezifischen Tastaturen schreibbar sind. Der Zugang zum Fragebogen wird bei sämtlichen Befragungen durch solche Passwörter geschützt, die den individuellen, persönlichen Fragebogen und die darin erfassten Daten schützt.
Administrator-Bereich und optional auch Ihre Befragungen werden mit der derzeit höchsten verfügbaren Secure Socket Layer Verschlüsselung (128/256 Bit permanente SSL Verschlüsselung) mit hochstehenden Cyphers vor fremden Einblicken auch via Sniffer-Software abgeschirmt. Wir nutzen zudem State-of-the-Art-Technologie auf Ebene Application Firewall und Intrusion Detection. Alle Datentransfers zwischen lokalem Rechner des Teilnehmers und unserer Datenbank sind damit verschlüsselt und mit derselben Verschlüsselung zerstückelt unterwegs, wie sie Banken und Versicherungen einsetzen, und können damit auf keinen Fall inhaltlich ausgelesen werden.
Weitere Massnahmen: Einschränkung der Zugriffe nur auf Daten, die von Mitarbeitenden gezielt für deren Aufgaben benötigt werden (Segmentierung), entsprechende Teilberechtigungen. Konsequente Minimierung von Akten in traditioneller Papier- und Notizform (Nutzung elektronisch geschützter Informationssysteme wie CRM, Wiki, Datenbanken). Eindeutige (persönliche) Zuweisung von Zugriffsberechtigungen mit persönlichem Passwörtern. Zuordnung von Verantwortlichkeiten. Automatisierte Prüfverfahren. Protokollierung der Systemnutzung. Verpflichtung der Mitarbeiter auf Datengeheimnis nach § 5 BDSG. Sämtliche Mitarbeitenden von onlineumfragen.com GmbH stehen zudem unter schriftlich und vertraglich vorliegenden Non Disclosure und Schweigepflichtsvereinbarungen, welche auch nach einem allfälligen Austritt aus unserem Unternehmen Gültigkeit bewahren und mit Konventionalstrafen ab 50‘000 Euro pro Einzelfall belegt sind. Verbot mobiler Datenträger wie USB-Sticks, CD’s, Speicherkarten. Die Sicherheit unserer Server-Systeme gegenüber externen ungewollten Zugriffen wird von mehreren zentralen Firewalls übernommen. Diese arbeiten nach dem Prinzip des Paketfilters, welcher einer demilitarized zone vorgeschaltet ist. Das Netzwerk selbst verfügt dabei selbst über einen sicheren privaten Adressbereich. Remotezugriffe für unsere Administratoren geschehen aus dem internen Netzwerk heraus lokal oder werden mit Protokollen mit Datenverschlüsselung (SSH) und weiteren Sicherheitsmassnahmen geschützt.

4. Weitergabekontrolle

   Modernste Sicherheitsmethoden für mobile Geräte wie Notebooks, Smartphones, etc. wie Fingerabdruckleser, Trusted Platform Modules, Verschlüsselte Festplatten. Getrennte Speicherplätze in Datenbanken für Antwort- und Kundendaten, zuverlässige erweiterte Löschverfahren (Löschsoftware). Vorschrift zur Verschlüsselung mit mindestens 128 Bit. Genaue Dokumentation unserer zwei beteiligten Rechenzentren. Protokollierung der Speicherorte von Daten. Sichere Übertragung zwischen den Rechenzentren (geschlossene Netze mit VPN SSL Verbindung, State of the Art Verschlüsselung).

5. Eingabekontrolle

   Login-/Logout-Protokolle mit IP, Browserangaben, Referer etc. Protokollierungsverfahren für alle Tätigkeiten unserer Mitarbeitenden inkl. Support. Protokollierung aller Bewegungen und Anpassungen durch den Kunden in dessen Admin-Bereich.

6. Auftragskontrolle

   Regelungen der Zweckbindung der Datennutzung durch den Auftraggeber sowie durch unsere Privacy Policy und AGB unter www.onlineumfragen.com/agb - Daten werden ausschliesslich zum vereinbarten Zweck verwendet (Erhebung, Versand, Durchführung, statistische Auswertung, Export für den Kunden). Daten können nach Aufforderung durch den Kunden unter Anfertigung

eines Löschprotokolls von unserer Seite jederzeit permanent gelöscht werden. Backup-Medien werden bis max. 1 Jahr nach Speicherdatum in einer Schweizer Bank gelagert und sind von der Löschung nur gegen Leistung eines entsprechend erhöhten Aufwands betroffen.

7. Verfügbarkeitskontrolle

   Siehe dazu auch unsere Broschüre „onlineumfragen_quickstart_sicherheit“. Wir unterhalten redundante, sichere Systeme mit regelmässiger Datensicherung und Anlagen zu Desaster Recovery, High Availability, Failover, mehrfach redundante Hochleistungs-Storages, unterbrechungsfreie Stromversorgung auf Enterprise-Level (USV), Inergen-Gas-Brandschutz-Anlage, Katastrophenplan (in der Schweiz gesetzlich vorgeschrieben), Regelung zur Gewährleistung des Zugriffs auf Daten (Service-Level 99,9%, best efford). Gegen Charge steht unser Pikett-Dienst 24h (365/7/99%) zur Verfügung. Wir überwachen unsere Systeme permanent mit Alert-Monitoren. Alle Serverdienste werden im Rahmen unseres Pikett-Dienstes mit verschiedenen Notszenarien und Eskalationsstufen ständig überprüft (24x7) und mögliche Systemunterbrüche proaktiv festgestellt und umgehend behoben.

8. Trennungskontrolle

   Trennung über Zugriffsregelung, Mandantentrennung, Dateiseparierung durch Ausgabe über Admin-Bereich (Onlinezugriff) in unterschiedlichen Accounts oder Multi-User-Zugriffen (getrennte Berechtigungen für verschiedene Daten / Umfragen).

[Stand 1.1.2017]/jj

Verantwortliche Stellen für die Einhaltung der Datenschutzbestimmungen sind bei onlineumfragen.com:

Josef Jutz, CEO
onlineumfragen.com GmbH
Untere Gründlistrasse 26
6055 Alpnach
Schweiz

Raffael Meier, CTO
Business Partner Datenschutz
onlineumfragen.com GmbH
Untere Gründlistrasse 26
6055 Alpnach
Schweiz

Datenschutzinformation für Umfrageteilnehmende

Was geschieht mit Ihren Angaben?

1. Die technischen Systeme bei onlineumfragen.com legen Ihre Angaben in einer sicheren Datenbank ab. Bei einer Onlineumfrage tragen Sie selbst Ihre Angaben in den Fragebogen am Bildschirm ein.

2. Bei onlineumfragen.com werden falls überhaupt vorhanden Adresse und Fragenteil getrennt. Daten und Adresse erhalten eine Code-Nummer und werden getrennt abgespeichert. Wer danach die Daten sieht, weiß also nicht, von wem die Angaben gemacht wurden. Die Adresse falls überhaupt vorhanden wird getrennt bis zum Projektende aufbewahrt, um Sie später im Rahmen dieser Untersuchung noch einmal aufsuchen oder anschreiben zu können. Bei Abschluss der Gesamtuntersuchung werden die Adressen gelöscht.

3. Die Daten des Fragenteils werden in Zahlen umgesetzt und ohne Ihre Adresse (also anonymisiert) in eine Auswertungsdatenbank gebracht.

4. Dann werden die Interviewdaten (ohne Adresse) von einem Computer ausgewertet. Der Computer zählt alle Antworten und errechnet beispielsweise Prozentergebnisse.

5. Das Gesamtergebnis und die Ergebnisse von Teilgruppen werden beispielsweise in Tabellenform ausgedruckt.

6. Es ist selbstverständlich, dass die beteiligten Institute alle Vorschriften des Datenschutzes einhalten. Sie können absolut sicher sein, dass

- Ihre Adresse nicht an Dritte weitergegeben wird.
- Keine Daten an Dritte weitergegeben werden, die eine Identifizierung Ihrer Person zulassen.

7. Bei der Befragung orientieren wir uns an Standards des Arbeitskreis Deutscher Markt- und Sozialforschungsinstitute e.V. (ADM)

Wir danken Ihnen für Ihre Mitwirkung und Ihr Vertrauen in unsere Arbeit!