«/Anlage technisch-organisatorische Massnahmen 2018»

Massnahmenbeschrieb
nach Art. 32 Abs. 1 DS-GVO (vormals §9 BDSG) bei onlineumfragen.com GmbH

Art. 32 DSGVO

1. Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen unter anderem Folgendes ein:

    a) die Pseudonymisierung und Verschlüsselung personenbezogener Daten;

    b) die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;

    c) die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;

    d) ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

2. Bei der Beurteilung des angemessenen Schutzniveaus sind insbesondere die Risiken zu berücksichtigen, die mit der Verarbeitung – insbesondere durch Vernichtung, Verlust oder Veränderung, ob unbeabsichtigt oder unrechtmäßig, oder unbefugte Offenlegung von beziehungsweise unbefugten Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden – verbunden sind.

3. Die Einhaltung genehmigter Verhaltensregeln gemäß Artikel 40 oder eines genehmigten Zertifizierungsverfahrens gemäß Artikel 42 kann als Faktor herangezogen werden, um die Erfüllung der in Absatz 1 des vorliegenden Artikels genannten Anforderungen nachzuweisen.

4. (...)

Anlage (zu Art. 32 DSGVO, aus §64 BDSG-neu)

Der Verantwortliche und der Auftragsverarbeiter haben unter Berücksichtigung des Stands der Technik, der Implementierungskosten, der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der Eintrittswahrscheinlichkeit und der Schwere der mit der Verarbeitung verbundenen Gefahren für die Rechtsgüter der betroffenen Personen die erforderlichen technischen und organisatorischen Maßnahmen zu treffen, um bei der Verarbeitung personenbezogener Daten ein dem Risiko angemessenes Schutzniveau zu gewährleisten, insbesondere im Hinblick auf die Verarbeitung besonderer Kategorien personenbezogener Daten. Der Verantwortliche hat hierbei die einschlägigen Technischen Richtlinien und Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik zu berücksichtigen.

Die in Absatz 1 genannten Maßnahmen können unter anderem die Pseudonymisierung und Verschlüsselung personenbezogener Daten umfassen, soweit solche Mittel in Anbetracht der Verarbeitungszwecke möglich sind. Die Maßnahmen nach Absatz 1 sollen dazu führen, dass

1. die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sichergestellt werden und
2. die Verfügbarkeit der personenbezogenen Daten und der Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederhergestellt werden können.

Im Fall einer automatisierten Verarbeitung haben der Verantwortliche und der Auftragsverarbeiter nach einer Risikobewertung Maßnahmen zu ergreifen, die Folgendes bezwecken:

1. Verwehrung des Zugangs zu Verarbeitungsanlagen, mit denen die Verarbeitung durchgeführt wird, für Unbefugte (Zugangskontrolle),
2. Verhinderung des unbefugten Lesens, Kopierens, Veränderns oder Löschens von Datenträgern (Datenträgerkontrolle),
3. Verhinderung der unbefugten Eingabe von personenbezogenen Daten sowie der unbefugten Kenntnisnahme, Veränderung und Löschung von gespeicherten personenbezogenen Daten (Speicherkontrolle),
4. Verhinderung der Nutzung automatisierter Verarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung durch Unbefugte (Benutzerkontrolle),
5. Gewährleistung, dass die zur Benutzung eines automatisierten Verarbeitungssystems Berechtigten ausschließlich zu den von ihrer Zugangsberechtigung umfassten personenbezogenen Daten Zugang haben (Zugriffskontrolle),
6. Gewährleistung, dass überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten mit Hilfe von Einrichtungen zur Datenübertragung übermittelt oder zur Verfügung gestellt wurden oder werden können (Übertragungskontrolle),
7. Gewährleistung, dass nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit und von wem in automatisierte Verarbeitungssysteme eingegeben oder verändert worden sind (Eingabekontrolle),
8. Gewährleistung, dass bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern die Vertraulichkeit und Integrität der Daten geschützt werden (Transportkontrolle),
9. Gewährleistung, dass eingesetzte Systeme im Störungsfall wiederhergestellt werden können (Wiederherstellbarkeit),
10. Gewährleistung, dass alle Funktionen des Systems zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden (Zuverlässigkeit),
11. Gewährleistung, dass gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden können (Datenintegrität),
12. Gewährleistung, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle),

13. Gewährleistung, dass personenbezogene Daten gegen Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle),

14. Gewährleistung, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden können (Trennbarkeit).

Ein Zweck nach Satz 1 Nummer 2 bis 5 kann insbesondere durch die Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren erreicht werden.

Massnahmen bei onlineumfragen.com (Stand 1.4.2018)

1. Zugangskontrolle

   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, Fingerabdruckkontrolle, Schlüssel, Personenvereinzelungsanlage, 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 (Closed Shop-Betrieb). Abschliessbare Serverschränke. Keine externen Servicepartner für Serverwartung). Backup-Medien in Bankschliessfach im Tresorraum einer Schweizer Bank. Serverräume mit redundanten Notstrom-Dieselgeneratoren und mehrfachredundanten Upstream-Provider (Carrier). Alle Räumlichkeiten von onlineumfragen.com verfügen über eine Alarmanlage. Reinigungspersonal ist nur während der Bürozeiten und bei Anwesenheit eines autorisierten OU-Mitarbeiters gestattet.

2. Datenträgerkontrolle

   Es werden keine mobilen Datenträger genutzt. Sämtliche Daten sind ausschliesslich auf verschlüsselt erreichbaren Laufwerken (SSL, VPN-Tunnel) in unserem Rechenzentrum gespeichert. Datenträger werden dokumentiert. Ausrangierte Datenträger werden ordnungsgemäss vernichtet und deren Vernichtung protokolliert.

3. Speicherkontrolle

   Alle Speichersysteme in unseren Rechenzentren sind durch Firewalls und Festlegung detaillierter Berechtigungen getrennt in separaten Subnetzen angelegt. Für Lesen, Löschen, Ändern existieren differenzierte Berechtigungen. Ebenso sind Berechtigungen nach System-Tiers wie Daten, Anwendungen und Betriebssystem festgelegt. Die Verwaltung der Rechte erfolgt ausschliesslich durch die Geschäftsleitung und deren direkt unterstellte Systemadministratoren. Für die Speichergeräte gilt eine Passwortrichtline (Policy) inkl. Länge, Komplexität und Passwortwechsel. Zugriffe und Traffic-Anomalien werden protokolliert und überwacht. Massnahmen und Systeme zur Datenverschlüsselung auf Datenträgern kommen zu Einsatz.

4. Benutzerkontrolle

   Passwortvergabe/-schutz aller wesentlichen technischen Systeme, Protokollierung der Nutzung aller wesentlichen technischen Systeme und Prozesse, Log-Kontrollen durch die Geschäftsleitung. Trennung über Zugriffsregelung, Mandantentrennung, Dateiseparierung durch Ausgabe über Admin-Bereich (Onlinezugriff) in unterschiedlichen Accounts oder Multi-User-Zugriffen (getrennte Berechtigungen für verschiedene Daten / Umfragen). Die nutzungsberechtigten Personen sind festgelegt und werden identifiziert und authentifiziert. Die Datenstationen, Netze und Übertragungsleitungen (z.B. Router, Firewalls) aller OU-Mitarbeitenden sind gesichert und verschlüsselt.

5. 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. Der Admin-Bereich kann zusätzlich kostenlos mittels Mehrfaktor-Authentifizierung per SMS geschützt werden, so dass Kunden nur auf ihre Daten zugreifen können, wenn sie auf ein autorisiertes Mobiltelefon zugreifen können. Alle Logins werden protokolliert.
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 persönlichen 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.

6. Übertragungskontrolle

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, Protokollierung, Statistiken über das detaillierte Traffic-Volumen, Anzahl und Zeitpunkt der Zugriffe, detaillierte Protokolle über den Zugriff auf Dateien).

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.

OU stellt zudem seinen Kunden sichere Upload- und Download-Möglichkeiten innerhalb des Admin-Bereichs und mittels spezieller eigener Online-Tools zur Verfügung. Eine sichere, SSL-verschlüsselte Übertragung von Daten auch grosser Volumen ist damit möglich. Dafür werden passwortbasiert Logdateien inkl. IP- und Agent-Informationen erstellt.

7. Eingabekontrolle

Login-/Logout-Protokolle mit IP, Browserangaben, Referer etc. Protokollierungsverfahren für alle Tätigkeiten unserer Mitarbeitenden inkl. Support. Login-/Logout-Protokolle mit IP, Browserangaben, Referer etc. Protokollierungsverfahren für alle Tätigkeiten der Nutzer der Online-Applikationen, inkl. Darstellung einer Login-History im Admin-Bereich. Protokollierung aller Bewegungen und Anpassungen des Kunden in dessen Admin-Bereich.

8. Transportkontrolle

Siehe Übertragungskontrolle. Ein physischer Transport von Daten findet nicht statt, mit Ausnahme einer Deponierung periodischer Backup-Medien in einem Bankschliessfach einer Schweizer Bank zum Zwecke Disaster Recovery durch ein Mitglied der Geschäftsleitung.

9. Wiederherstellbarkeit

Es liegt ein Disaster Recovery-Konzept vor, welches von der Geschäftsleitung bewirtschaftet wird. OU setzt ausschliesslich mehrfach redundante Speichersysteme ein (mehrfach gespiegelte Festplatten, hochredundante Storage-Server, mehrfachredundante Switches und Firewalls). Sämtliche produktiven Systeme sind bei OU so angelegt, dass ein Ausfall einer Komponente keinen Dienstleistungsunterbruch erzeugen kann. Die Massnahmen zur Datenwiederherstellung sowie Wiederherstellung aller einzelnen Komponenten werden regelmässig getestet. Es werden Staging-Server-Systeme regelmässig aufgesetzt, um die Inbetriebnahme einer parallelen Infrastruktur im Notfall umsetzen zu können.

10. Zuverlässigkeit

Unsere Software und alle Core-Komponenten wie WebServer, Datenbankserver, Applikationsserver, Mailserver, Dateiserver, VPN, Firewalls, Backup-Server, werden permanent überwacht und Fehlfunktionen, Störungen und Warnungen protokolliert. Solche Meldungen werden automatisch den zuständigen Personen bei OU sichtbar gemacht. Auf allen Dateisystemen sind Anti-Virus-Programme im Einsatz. Wir betreiben unabhängig parallele Systeme, um im Bedarfsfall alternative Komplettsysteme zum Einsatz zu bringen.

11. Datenintegrität

Es liegt ein Disaster Recovery-Konzept vor, welches auf verschiedenen Ebenen Backup- und Wiederherstellungsszenarien abdeckt, z.B. Wiederherstellung von Storage-Systemen, von Server-Systemen, von Datei-Systemen oder von Datenbanken.

12. Auftragskontrolle

Onlineumfragen.com beschäftigt im Bereich der Verarbeitung von Personendaten keinerlei Subunternehmen und vergibt für die Verarbeitung keine Aufträge. Alle weiteren externen Dienstleister die im Rahmen von Kundenprojekten Kundendaten verarbeiten, wie z.B. zum Zwecke der Buchhaltung, der Druckdienstleistung bei Papier-und-Bleistift-Fragebögen, Versanddienstleister wie UPS oder die Post, werden vollumfänglich zur Geheimhaltung und zur Einhaltung der Vorschriften nach DS GVO verpflichtet.

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.

13. 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). Überwacht werden in unseren Data-Centern direkt auf unseren Servern Temperatur, Feuchtigkeit, Stromverbraucht und Traffic der Uplinks. Off-Site-Backups werden zwischen unseren Data-Centern erstellt. 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.

14. Trennbarkeit

Trennung über Zugriffsregelung, Mandantentrennung, Dateiseparierung durch Ausgabe über Admin-

Bereich (Onlinezugriff) in unterschiedlichen Accounts oder Multi-User-Zugriffen (getrennte Berechtigungen für verschiedene Daten / Umfragen).

15. Organisationskontrolle

Als Schweizer Unternehmen sind wir dem Schweizer Datenschutzgesetz (DSG) unterstellt. Zusätzlich unterstellen wir uns DS GVO bezogenen Verpflichtungen mittels zusätzlicher Vereinbarungen und Datenschutzverträgen (wie z.B. NDA, Vertrag zur Auftragsverarbeitung gemäß Art. 28 Datenschutz-Grundverordnung, usw.) und unserem Commitment zu den technisch-organisatorischen Massnahmen auf Basis der EU DS GVO.

Onlineumfragen.com bestellt dazu einen betrieblichen Datenschutzverantwortlichen nach Schweizer Recht, der die datenschutzbezogenen operativen, organisationalen und technischen Ziele umsetzt und einen externen Datenschutzbeauftragten nach deutschem Recht entsprechend DS GVO, welcher auf eine Umsetzung aller datenschutzrelevanter Aspekte gemäss DS GVO hinwirkt und an dessen Instruktionen der betriebliche Datenschutzverwortliche eng gebunden ist.

Alle wesentlichen Systemerweiterungen, -anpassungen, neue Software und Systeme werden eingehend mittels Freigabeverfahren (Testsystem, Stagingsystem, Produktivsystem) durch die Geschäftsleitung eingeführt. Programmierrichtlinen für sicheren Code (Schaden verhindern, Müll entfernen, client-validation, server-validation, server-sanitation, indirect database objects), Vorgaben für die Dokumentation von Code, periodische Schulung aller Mitarbeitenden zu Datenschutzthemen, Notfallkonzept, regelmässige Datensicherung, Process Manual für Mitarbeitende, zentrale Beschaffung der Hard- und Software durch die Geschäftsleitung, regelmässige interne Audits zur Daten- und WebSite-Sicherheit, regelmässige externe Nachweise und Testings zur IT- und Datensicherheit.

[Stand 1.4.2018]/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
Datenschutzverantwortlicher

onlineumfragen.com GmbH
Untere Gründlistrasse 26
6055 Alpnach
Schweiz

Datenschutzinformation für Umfrageteilnehmende bei anonymisierten Umfragen (mit Anonymitätssiegel)

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 Antwortdaten 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!

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