Anlage
technische & organisatorische Massnahmen

nach Art. 32 Abs. 1 DS-GVO sowie Art. 8 Abs. 1 DSG Schweiz
bei onlineumfragen.com GmbH, Kernserstrasse 15, 6056 Kägiswil

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).

Maßnahmen bei onlineumfragen.com (Stand 16.1.2024)

Um das nach Artikel 32 DSGVO geforderte angemessene Schutzniveau zu gewährleisten, und einen einwandfreien, hochverfügbaren und performanten Betrieb unserer Systeme sicher zu stellen, trifft die onlineumfragen.com GmbH folgende umfassenden und über die gesetzlichen Anforderungen hinausreichenden Maßnahmen:

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 Kägiswil 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 mit Applikations-Source-Code 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. Sämtliche Besucher sind nur in Gegenwart und Begleitung unserer Mitarbeiter zugelassen.

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 (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 den Ebenen Edge-Firewalls, 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. 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. Für die Entsorgung von dennoch anfallenden Papieren und Dokumenten verwenden wir sichere Aktenschredder der Stufe 3. Allfällig zu löschende Datenträger werden im Office-Bereich mit Überschreibsoftware gelöscht. Sämtliche Benutzerrechte in Zusammenhang mit Mitarbeitenden der onlineumfragen.com GmbH werden von der GL (CTO) verwaltet und protokoliert. Weitere Massnahmen sind: Anweisung an Mitarbeiter, nicht in öffentlich zugänglichen Räumlichkeiten (z.B. Cafés) zu arbeiten; Arbeit im Home Office: Anweisung an Mitarbeiter, wenn möglich, in von Wohnräumen abgetrennten Arbeitszimmer zu arbeiten; Sorgfältige Auswahl des Reinigungspersonals für unsere Büroräume (Reinigung nur in Anwesenheit von Mitarbeitenden); Unternehmensrichtlinie „CleanDesk“.

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 (256 Bit permanente SSLVerschlüsselung) 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. Unsere RTO (Recovery Time Objective, Zeit, bis Systeme wiederhergestellt werden können) für alle Produktivsysteme liegt bei 2h (Worst Case). Unsere RPO (Recovery Point Objective, Zeit zwischen zwei Datensicherungen) liegt für Datenbanken unter 2 Minuten, für Kundendateien wie hochgeladene Bilder in Umfragen bei 24h. Unsere Infrastrukturen sind mehrfach redundant angelegt, so dass allfällige Ausfälle in der Regel von Aussen nicht wahrnehmbar sind.

10. Zuverlässigkeit

Unsere Software und alle Core-Komponenten wie WebServer, Reverse Proxys, Firewalls, Datenbankserver, Applikationsserver, Mailserver, Dateiserver, VPN, Backup-Server, Storage-Cluster 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 effort). 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-Monitoring. 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, Staging-System, 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 Settings zur IT- und Datensicherheit.

16. Pseudonymisierung *(Art. 32 Abs. 1a DSGVO; Art. 25 Abs. 1 DSGVO)*

In bestimmten Kontexten, wo technisch und wirtschaftlich möglich, werden Daten pseudonymisiert, also so verwaltet, dass Daten nicht mehr einer spezifischen Person zugeordnet werden können, ohne einen zusätzlichen Pseudonymisierungskontext hinzuzuziehen (Reverse Engineering).

Im Falle der Technologie des Ersetzens von Personendaten durch geeignete Merkmale wie User-ID, UID, gehashte Passwörter oder Buchstaben- und Zahlenkombinationen (z.B. in unserer Datenbank) ist ein Reverse Engineering nur möglich, wenn gesondert aufbewahrte zusätzliche Informationen wie Verbindungsschlüssel oder sogenannte Primary und Foreign Keys beigezogen werden. Diese gesonderten Informationen unterliegen ebenfalls unseren technisch-organisatorischen Maßnahmen. Im Falle der Technologie des Hashing (z.B. unsere Systemfunktionen zum sogenannten DSGVO-Hashing von E-Mail-Adressen oder anderen Personendaten) werden Daten so pseudonymisiert, dass diese mittels eines kryptologischen Algorithmus verschlüsselt werden, in einem Verfahren, welches ein Reverse Engineering ausschließt, und gleichzeitig für gleiche Daten gleiche gehashte (eindeutige) Werte erzeugt. Dies ermöglicht zum Beispiel, Auswertungen nach verschiedenen Abteilungen auch dann noch berechnen zu können, wenn die Abteilungen selbst (im Wortlaut) durch Hashing unleserlich (verschlüsselt) wurden. Jeder Abteilung ist dann ein eindeutiger, unterschiedlicher und pro Abteilung immer gleicher Hash-Wert zugeordnet, der die Eigenschaft der Eindeutigkeit nach wie vor erfüllt, aber keinen Rückschluss auf die Abteilung an sich zulässt.

16. Verfügbarkeit und Belastbarkeit *(Art. 32 Abs. 1b DSGVO)*

Onlineumfragen.com setzt im Interesse der eigenen Geschäftskontinuität IT-Systeme für die Betreibung des Online-Tools und aller Kundensysteme ein, die in Bezug auf Verfügbarkeit und Belastbarkeit sehr hohe Anforderungen erfüllen. In erster Linie sind dies Eigenschaften der IT-Umgebung und Anbindung in unserem Rechenzentrum wie redundante Stromversorgung (auf Ebene Stromanbieter und auf Ebene Rackversorgung), mehrfach redundante Server-Systeme (sowohl auf Hardware- wie auch auf Softwarebene), mehrfach redundante Storage-Systeme, permanente Onsite- und Offsite-Backups, Disaster-Recovery in-place mit regelmässigen Tests. Bei einer Verfügbarkeit von mehr als 99.95% in den letzten 5 Jahren insgesamt und auch in den einzelnen Jahren 2014 bis 20222 und der Möglichkeit für unsere Kunden, Service-Level-Agreements abzuschliessen, übertreffen oder erreichen wir das gesetzlich nur allgemein gehaltene Ziel der Verfügbarkeit im Rahmen vergleichbarer Online-Dienstleister deutlich. Die Belastbarkeit unserer Systeme wird regelmässig getestet, dabei setzen wir Tools wie Apache JMeter, Akamai, Locust, Alertra, und weitere ein. Testmetriken sind Latenz, Seitenladezeit, Durchsatz, maximale Requests pro Sekunde, Database slow queries. Regelmässige Loganalysen ergänzen diese Tests, um Spitzenbelastungen und Tendenzen im Live-Betrieb zu identifizieren.

Belastbarkeit wird bei onlineumfragen.com als klassisches Ziel einer leistungsfähigen IT-Infrastruktur betrachtet. Als Standbeine bezeichnen wir Resilienz und Robustheit. Letztere wird durch State-of-the-Art-Verfahren wie Firewalls (pfSense vor sämtlichen Systemen und zwischen privaten Netzwerkübergängen, sowie zwei permanent aktive Application Level Firewalls), Intrusion Prevention Software wie snort, surricata, etc. und der Anwendung der OWASP Best Practice sowie regelmässigen Updates und Patches exponierter Dienste erreicht. Zudem setzen wir ausschliesslich bewährte

führende Netzwerktechnologien an Edge-Positionen ein wie z.B. Cisco oder DELL Switches, die über stabile Abwehrmechanismen verfügen.

Resilienz wird durch die permanente Verfügbarkeit von Ersatzsystemen und parallelen Infrastrukturen erreicht, die in Fällen unvorhersehbarer Ereignisse in sehr kurzer Zeit (Stunden) einsatzbereit sind (durch Ersatzgeräte, Ersatzsysteme, Backups, Virtualisierung und Nutzung externer Dienste wie DNS und Überwachungsserver). Zudem setzen wir adaptive Systeme ein, die aus Vorfällen lernen und Regeln zur Absicherung von Systemen selbständig erweitern.

16. Regelmäßige Überprüfung, Bewertung und Evaluierung der Wirksamkeit *(Art. 32 Abs. 1d DSGVO)*

Onlineumfragen.com hat die Fragen des Datenschutzes und der Weiterentwicklung der technisch-organisatorischen Maßnahmen im Sinne einer kontinuierlichen Anpassung an die naturgemäßen Weiterentwicklungen in der IT Branche zum Geschäftsleitungsthema erklärt. Wir betreiben ein Incident-Management (Einsatz von Firewalls, IDS, IPS, Spamfilter, Virenscanner inkl. regelmässige Aktualisierung), sowie ein Datenschutz-Management.

Ein dokumentierter Prozess zur Erkennung und Meldung von Sicherheitsvorfällen und Datenpannen ist definiert. Alle Sicherheitsvorfälle werden durch unsere IT bearbeitet, dokumentiert und der Geschäftsführung gemeldet. Allfällig betroffene Auftraggeber werden umgehend über Zeitpunkt, Art und Umfang informiert. Zudem erheben wir im Sinne von „Privacy by default“ nicht mehr personenbezogene Daten, als für den jeweiligen Zweck erforderlich sind und/oder durch den Auftraggeber beauftragt worden sind. Alle unsere Umfragen enthalten zudem die Möglichkeit für Teilnehmende, per Mausklick die Datenschutzrichtlinien aufzurufen – dort ist eine Ausübung des Widerrufsrechts resp. das Ausüben des Rechts auf Vergessen möglich.

Unsere Mitarbeitenden werden im Bereich „Privacy by design“ und „Privacy by default“ regelmässig geschult. Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck notwendig sind.

Sämtliche TOM werden je nach Maßnahme mindestens jährlich einzeln durch die Geschäftsleitung oder im Auftrag der Geschäftsleitung überprüft. Bestimmte Maßnahmen erfordern eine regelmäßigere oder permanente Überwachung, die auch im Interesse der Aufrechterhaltung und Performanz unserer geschäftskritischen Services liegt. Beispielsweise werden unsere Firewalls täglich geprüft oder unsere Server-Middleware und Java-Instanzen wöchentlich gepatched und auf den neusten Stand gebracht. Auch unsere Datenbanken unterliegen einer durchgehenden 24h-Kontrolle und Überwachung durch elektronische Überwachungstools, die Auffälligkeiten jederzeit an unsere IT melden. Die Prüfintervalle sind also pro Maßnahme unterschiedlich.

Jährliche Schulungen sämtlicher Mitarbeitenden bei onlineumfragen.com stellen sicher, dass aktuelle Datenschutzthemen auch auf Ebene Mitarbeitende bekannt sind. Alle Mitarbeitenden sind zudem auf Vertraulichkeit und Datengeheimnis vertraglich verpflichtet.

Ein formalisierter Prozess zur Bearbeitung von Auskunftsanfragen seitens Betroffener ist definiert.

Das Thema Auftragskontrolle ist für unser Unternehmen nicht maßgebend, da wir keinerlei Subunternehmen in Zusammenhang mit personenbezogenen Daten einsetzen.

17. Datenschutz-Management

Folgende Maßnahmen sollen gewährleisten, dass eine den datenschutzrechtlichen Grundanforderungen genügende Organisation vorhanden ist:
- Verwendung der heyData-Plattform zum Datenschutz-Management
- Stellung des Datenschutzberaters durch heyData
- Verpflichtung der Mitarbeiter auf das Datengeheimnis
- Regelmäßige Schulungen der Mitarbeiter im Datenschutz
- Führen eines Verzeichnisses über Bearbeitungstätigkeiten (Art. 12 DSG)

18. Incident-Response-Management

- Meldeprozess für Datenschutzverletzungen nach Art. 5 lit. h DSG gegenüber dem EDÖB (Art. 24 Abs. 1 DSG)
- Meldeprozess für Datenschutzverletzungen nach Art. 5 lit. h DSG gegenüber betroffenen Personen (Art. 24 Abs. 4 DSG)
- Einbindung des Datenschutzberaters in Sicherheitsvorfälle und Datenpannen
- Einsatz von Anti-Viren-Software
- Einsatz von Firewalls auf mehreren Ebenen (Application, Network, Edge)

16.1.2024

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

Datenschutzberater nach DS-GVO:
heyData GmbH, Schützenstraße 5,
10117 Berlin, www.heydata.eu, E-Mail: datenschutz@heydata.eu

Raffael Meier
Datenschutzverantwortlicher
onlineumfragen.com GmbH
info@onlineumfragen.com