Vertrag
zur Datenverarbeitung im Auftrag gemäß Art. 28 EU-Datenschutz-Grundverordnung (DSGVO)

zwischen

LamaPoll
Lamano GmbH & Co. KG
Prenzlauer Allee 36 G, 10405 Berlin
www.lamapoll.de

- nachstehend ***Auftragnehmer*** genannt -

und

……

……

……

- nachstehend ***Auftraggeber*** genannt -

1. Präambel

Dieser Datenschutzvertrag regelt den Schutz personenbezogener Daten bei der Datenverarbeitung im Auftrag. Lässt eine verantwortliche Stelle (Auftraggeber) die Verarbeitung von personenbezogenen Daten durch eine andere Stelle (Auftragnehmer) ausführen, ist gemäß Art. 28 DSGVO ein schriftlicher Vertrag zur Auftragsverarbeitung abzuschließen.

Sofern in diesem Vertrag der Begriff „Datenverarbeitung“ oder „Verarbeitung“ (von Daten) benutzt wird, wird die Definition der „Verarbeitung“ i.S.d. Art. 4 Nr. 2 DSGVO zugrunde gelegt: zur Datenverarbeitung zählt neben dem Speichern, Verändern, Übermitteln, Sperren und Löschen auch das Bereithalten von Daten zur Einsicht oder zum Abruf durch einen Dritten.

Die Verantwortung für die datenschutzkonforme Verarbeitung der personenbezogenen Daten verbleibt beim Auftraggeber. Nach Art. 29 DSGVO darf der Auftragnehmer die Daten nur auf Weisung des Auftraggebers verarbeiten. Verstößt der Auftragnehmer dagegen, indem er z.B. Zwecke der Verarbeitung selbst bestimmt, wird er nach Art. 28 Abs. 10 DSGVO gegenüber Betroffenen selbst zum Verantwortlichen.

Aus diesem Grunde regeln die Parteien Folgendes:

2. Gegenstand und Dauer des Auftrags

2.1. Gegenstand des Auftrags (Art. 28 Abs. 3 S. 1 DSGVO)

Zutreffendes bitte ankreuzen und ausfüllen.

Gegenstand des Auftrags (Leistungsbeschreibung) zum Datenumgang ist die Durchführung folgender Aufgaben:

Bspw. Durchführung von Online Umfragen zum Zwecke.. Übermittlung der E-Mail-Adressen von.. zum Versand.. Erhebung und Erfassung…

……..

……..

……..

……..

……..

……..

2.2. Dauer des Auftrags

Das Vertragsverhältnis tritt mit Unterzeichnung durch beide Vertragspartner in Kraft. Wenn die Grundlagen der Vertragserfüllung wesentlich verändert werden oder ganz entfallen aufgrund einer Änderung der Rechts- oder Gesetzeslage oder eines Eingreifens oder einer sonstigen Maßnahme der aufsichtführenden Behörden, haben beide Parteien einen Anspruch auf Anpassung des Vertrages an die neuen Verhältnisse, soweit dies möglich und für beide Parteien zumutbar ist. Ist eine Vertragsanpassung nicht möglich oder für eine Partei unzumutbar, ist dies für beide Parteien ein wichtiger Grund für eine fristlose Kündigung.

☐ Der Auftrag ist unbefristet erteilt.

☐ Die Dauer der Verarbeitung beginnt am …… und ist befristet bis zum …….

3. Weisungsbefugte Personen des Auftraggebers

Bitte mindestens 2 Vertretungsbefugte benennen:

Name	E-Mail	Telefon
……	……	……
……	……	……
……	……	……

Für den Fall, dass sich die weisungsberechtigten Personen beim Auftraggeber ändern, wird der Auftraggeber dies dem Auftragnehmer schriftlich oder in Textform mitteilen.

4. Konkretisierung des Auftragsinhalts:

4.1. Ort der Verarbeitung

Die Verarbeitung und Nutzung der Daten findet ausschließlich auf dem Gebiet der Bundesrepublik Deutschland statt.

4.2. Art der Verarbeitung

Laut Art. 4 Nr. 2 DS-GVO betrifft "Verarbeitung" jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

Die Art der Verarbeitung umfasst alle Arten von Verarbeitungen im Sinne der DSGVO zur Erfüllung des Auftrags, insbesondere:

- Speichern, Löschung
- Offenlegung im Backend, Übermittlung durch Export
- Organisieren, Ordnen, math. Berechnungen der Daten bei Auswertung

4.3. Art der Daten (Art. 4 Nr. 1, 13, 14 und 15 DSGVO):

Gegenstand der Erhebung, Verarbeitung und/oder Nutzung der personenbezogenen Daten sind folgende Daten bzw. Datenkategorien: **(Bitte ankreuzen oder ergänzen)**

☐ Name, Titel, akademischer Grad

☐ Anschrift

☐ Geburtsdatum

☐ Personalstammdaten

☐ Kommunikationsdaten (z.B. Telefon, E-Mail)

☐ Besondere Arten personenbezogener Daten (Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben, biometrische Daten, genetische Daten, Daten zu strafrechtlichen Verurteilungen und Straftaten)

☐ ……..

☐ ……..

☐ ……..

4.4. Kreis der Betroffenen (Art. 4 Nr. 1 DS-GVO)

Der Kreis der durch den Umgang ihrer personenbezogenen Daten im Rahmen dieses Auftrags Betroffenen ist: **(Bitte ankreuzen oder ergänzen)**

☐ Kunden

☐ Beschäftigte

☐ Mitglieder

☐ Bewerber

☐ Lieferanten

☐ ……

☐ ……

☐ ……

5. Technische und organisatorische Maßnahmen (Art. 28 Abs. 3 S. 3 lit. c DSGVO)

Der Auftragnehmer hat die im Vorfeld der Auftragsvergabe dargelegten technischen und organisatorischen umgesetzten Maßnahmen vor Beginn der Verarbeitung zu dokumentieren und dem Auftraggeber zur Prüfung zu übergeben. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Auftrags.

Insgesamt handelt es sich bei den zu treffenden Maßnahmen um solche, welche die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung personenbezogene Daten sicherstellen; Maßnahmen, welche die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherstellen sowie Maßnahmen, welche durch regelmäßige Überprüfungen, Bewertungen und Evaluierungen die Wirksamkeit dieser Maßnahmen gewährleistet.

Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren und dem Auftraggeber auf Anfrage zur Verfügung zu stellen.

Für die technischen und organisatorischen Maßnahmen **siehe Anlage 1: Darstellung der technischen und organisatorischen Sicherheitsmaßnahmen.**

6. Berichtigung, Sperrung und Löschung von Daten

a) Der Auftraggeber ist für die Wahrung der Betroffenenrechte allein verantwortlich.

b) Der Auftragnehmer hat nur nach Weisung des Auftraggebers die Daten, die im Auftrag verarbeitet werden, zu berichtigen, zu löschen oder zu sperren.

c) Wendet sich eine betroffene Person mit Forderungen zur Berichtigung, Löschung oder Auskunft an den Auftragnehmer, wird der Auftragnehmer die betroffene Person an den Auftraggeber verweisen, sofern eine Zuordnung an den Auftraggeber nach Angaben der betroffenen Person möglich ist. Der Auftragnehmer leitet den Antrag der betroffenen Person unverzüglich an den Auftraggeber weiter. Der Auftragnehmer unterstützt den Auftraggeber im Rahmen seiner Möglichkeiten auf Weisung. Der Auftragnehmer haftet nicht, wenn das Ersuchen der betroffenen Person vom Auftraggeber nicht, nicht richtig oder nicht fristgerecht beantwortet wird.

d) Auskünfte an Dritte oder die betroffene Person darf der Auftragnehmer nur nach vorheriger schriftlicher Zustimmung durch den Auftraggeber erteilen.

7. Allgemeine Pflichten des Auftragnehmers

a) Der Auftragnehmer bestätigt, dass er einen betrieblichen Datenschutzbeauftragten nach Art. 37 DSGVO benannt hat.

b) Die Pflicht, alle Personen, die auftragsgemäß auf personenbezogene Daten des Auftraggebers zugreifen können, zur Vertraulichkeit zu verpflichten (Art. 28 Abs. 3 S. 2 lit. b) DSGVO) und über die sich aus diesem Auftrag ergebenden besonderen Datenschutzpflichten sowie die bestehende Weisungs- bzw. Zweckbindung zu belehren.

c) Die Pflicht zur Umsetzung und Einhaltung aller für diesen Auftrag notwendigen technischen und organisatorischen Maßnahmen entsprechend Art. 32 DSGVO (vgl. Art. 28 Abs. 3 S. 2 lit. c) DSGVO).

d) Die Pflicht, erforderliche technischen und organisatorischen Maßnahmen zu ergreifen, damit der Auftraggeber die Rechte der betroffenen Personen nach Kapitel III der DSGVO (Information, Auskunft, Berichtigung und Löschung, Datenübertragbarkeit und Widerspruch sowie automatisierte Entscheidungsfindung im Einzelfall) erfüllen kann. Dazu überlässt der Auftragnehmer dem Auftraggeber alle dafür notwendigen Informationen. Dies setzt voraus, dass der Auftraggeber den Auftragnehmer hierzu schriftlich angewiesen hat und die Unterstützung nicht gegen Verschwiegenheitsverpflichtungen des Auftragnehmers gegenüber Dritten verstößt. Der Auftragnehmer behält sich vor, dadurch entstandene Kosten dem Auftraggeber gesondert in Rechnung zu stellen.

e) Im Hinblick auf die Kontrollverpflichtungen des Auftraggebers nach Art. 28 Abs. 1 DSGVO vor Beginn der Datenverarbeitung und während der Laufzeit des Auftrags stellt der Auftragnehmer sicher, dass sich der Auftraggeber von der Einhaltung der getroffenen technischen und organisatorischen Maßnahmen überzeugen kann. Hierzu weist der Auftragnehmer dem Auftraggeber auf Anfrage die Umsetzung der technischen und organisatorischen Maßnahmen gemäß Art. 32 DSGVO nach. Dabei kann der Nachweis der Umsetzung solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, auch durch Vorlage eines aktuellen Testats, von Berichten oder Berichtsauszügen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren) oder einer geeigneten Zertifizierung durch ein IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz) oder durch die Einhaltung genehmigter

Verhaltensregeln (sogenannte BCR) erbracht werden. Der Auftragnehmer behält sich vor, dadurch entstandene Kosten dem Auftraggeber gesondert in Rechnung zu stellen.

f) Die Pflicht, den Auftraggeber bei der Einhaltung der in Art. 32 bis 36 DSGVO genannten Pflichten (Datensicherheitsmaßnahmen, Meldungen von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde, Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person, Datenschutz-Folgenabschätzung, vorherige Konsultation) zu unterstützen (vgl. Art. 28 Abs. 3 S. 2 lit. f) DSGVO).

g) Die Pflicht zur unverzüglichen Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde (vgl. Art. 31, 51ff. DSGVO). Dies gilt auch, soweit eine zuständige Behörde nach Art. 83, 84 DSGVO beim Auftragnehmer ermittelt.

8. Rechte und Pflichten des Auftraggebers

a) Der Auftraggeber ist verantwortliche Stelle bzw. Verantwortlicher i.S.d. Art. 4 Nr. 7 DSGVO für die Verarbeitung von Daten im Auftrag durch den Auftragnehmer.

b) Dem Auftragnehmer steht das Recht zu, den Auftraggeber auf seiner Meinung nach rechtlich unzulässige Datenverarbeitungen hinzuweisen. Sofern der Auftragnehmer darlegen kann, dass eine Verarbeitung nach Weisung des Auftraggebers zu einer Haftung des Auftragnehmers nach Art. 82 DSGVO führen kann, steht dem Auftragnehmer das Recht frei, die weitere Verarbeitung insoweit bis zu einer Klärung der Haftung zwischen den Parteien auszusetzen.

c) Der Auftraggeber ist als verantwortliche Stelle / Verantwortlicher für die Wahrung der Betroffenenrechte verantwortlich. Der Auftragnehmer wird den Auftraggeber unverzüglich darüber informieren, wenn Betroffene ihre Betroffenenrechte gegenüber dem Auftragnehmer geltend machen.

d) Der Auftraggeber hat sich vor Beginn der Datenverarbeitung und sodann regelmäßig von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zur Datensicherheit zu überzeugen. Hierbei hat der Auftraggeber das Recht, auf eigene Kosten, die Auftragskontrollen im Vernehmen mit dem Auftragnehmer zu üblichen Geschäftszeiten, ohne Störung des Betriebsablaufes durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen, sofern diese nicht in einem Wettbewerbsverhältnis mit dem Auftragnehmer stehen oder andere berechtigte Gründe seitens des Auftragnehmers dem entgegenstehen. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die zur Wahrung seiner Verpflichtung zur Auftragskontrolle erforderlichen Auskünfte zu geben und die entsprechenden Nachweise verfügbar zu machen.

e) Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten im Zusammenhang mit der Verarbeitung personenbezogener Daten durch den Auftragnehmer feststellt.

f) Für den Fall, dass eine Informationspflicht gegenüber Dritten nach § 42a BDSG, § 15a TMG, § 109a TKG oder Art. 33, 34 DSGVO besteht, ist der Auftraggeber für deren Einhaltung verantwortlich.

9. Unterauftragsverhältnisse

Der Auftragnehmer bedient sich zur Vertragserfüllung dem folgenden Unterauftragnehmer:

Aufgabe: Serverhosting

Unterauftragnehmer: STRATO AG · Pascalstraße 10 · 10587 Berlin

Der Auftraggeber ist damit einverstanden, dass der Auftragnehmer für die Verarbeitung personenbezogener Daten des Auftraggebers die hier aufgezählten Unterauftragnehmer einsetzt.

Der Auftraggeber gestattet die Beauftragung weiterer Unterauftragnehmer ohne vorherige gesonderte Genehmigung. Der Auftragnehmer informiert den Auftraggeber vorab über jede beabsichtigte Beauftragung weiterer Unterauftragnehmer oder die Änderung bestehender Beauftragungen. Der Auftraggeber hat gegen die Beauftragung neuer Unterauftragnehmer oder die Änderung bestehender Beauftragungen ein Recht zum Einspruch.

Soweit mit der Verarbeitung oder Nutzung personenbezogener Daten des Auftraggebers weitere Unterauftragnehmer einbezogen werden, wird dies grundsätzlich nur unter folgenden Voraussetzungen genehmigt:

a) Durch die Einschaltung weiterer Unterauftragnehmer muss das Schutzniveau der personenbezogenen Daten mindestens gleich bleiben oder erhöht werden.

b) Nimmt der Auftragnehmer die Dienste eines weiteren Unterauftragnehmers für die Verarbeitung personenbezogener Daten des Auftraggebers in Anspruch, so erlegt er dem Unterauftragnehmer vorab dieselben Datenschutzpflichten auf, die zwischen ihm und dem Auftraggeber in dieser Vereinbarung festgelegt sind. Er stellt dabei insbesondere sicher, dass der Unterauftragnehmer hinreichende Garantien bietet, dass geeignete technische und organisatorische Maßnahmen getroffen sind und so durchgeführt werden, dass die Verarbeitung entsprechend den Anforderungen des Datenschutzrechts und dieser Vereinbarung erfolgt. Der Auftragnehmer haftet dem Auftraggeber für die Einhaltung dieser Datenschutzpflichten durch den Unterauftragnehmer.

c) Der Standort der Verarbeitung der personenbezogenen Daten darf nicht außerhalb der Europäischen Union verlagert werden.

Nicht als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Leistungen zu verstehen, die der Auftragnehmer bei Dritten als Nebenleistung zur Unterstützung bei der Auftragsdurchführung in Anspruch nimmt. Dazu gehören beispielsweise Reinigungsleistungen, reine Telekommunikationsleistungen ohne konkreten Bezug zu Leistungen, die der Auftragnehmer für den Auftraggeber erbringt, Post- und Kurierdienste, Transportleistungen, Bewachungsdienste. Der Auftragnehmer ist gleichwohl verpflichtet, auch bei Nebenleistungen, die von Dritten erbracht werden, Sorge dafür zu tragen, dass angemessene Vorkehrungen und technische und organisatorische Maßnahmen getroffen wurden, um den Schutz personenbezogener Daten zu gewährleisten. Wartung und Prüfung von IT-Systemen stellen zustimmungspflichtige Unterauftragsverhältnisse dar, soweit solche IT-Systeme betroffen sind, die für die Erbringung der Leistungen für den Auftraggeber erforderlich sind.

10. Beendigung

Die Dienstleistung des Auftragnehmers kann pausiert und zu einem späteren Zeitpunkt wiederholt oder wiederaufgenommen werden. Es erfolgt keine automatische Löschung der Daten nach Abschluss der Verarbeitung oder nach Beendigung dieses Vertrages.

Der Auftraggeber hat jedoch jederzeit die Möglichkeit, sämtliche personenbezogene Daten selbst zu löschen. Nach Löschung der Daten verbleiben diese bis zu 7 weitere Tage verschlüsselt beim Auftragnehmer und werden im Anschluss unwiederbringlich gelöscht. Unberührt bleiben Daten sowie Kopien, die zur Erfüllung von Haftungs- und Gewährleistungsansprüchen erforderlich sind.

Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, oder aus Rechtsgründen, z.B. wegen bestehender Aufbewahrungsfristen, nicht gelöscht werden dürfen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren.

11. Sonstiges

Ergänzungen und Änderungen dieses Vertrags bedürfen der Schriftform.

Erweist sich eine Bestimmung dieses Vertrages als unwirksam, so berührt dies die Wirksamkeit der übrigen Bestimmungen des Vertrags nicht. Beide Vertragsparteien sind in diesem Falle verpflichtet, unverzüglich in eine nachträgliche Zusatzbestimmung einzuwilligen, die nach Sinn und Zweck der unwirksamen Bestimmung am nächsten kommt.

Alleiniger Gerichtsstand für alle Streitigkeiten aus und im Zusammenhang mit dieser Vereinbarung ist, vorbehaltlich eines etwaigen ausschließlich gesetzlichen Gerichtsstandes, Berlin. Beide Seiten bleiben jedoch zur Erhebung der Klage oder der Einleitung sonstiger gerichtlicher Verfahren am allgemeinen Gerichtsstand bzw. Sitz der jeweiligen Gesellschaft berechtigt.

12. Anlagenverzeichnis

Anlage 1: Darstellung der technischen und organisatorischen Sicherheitsmaßnahmen gemäß Art. 32 DSGVO

Ort, Datum	Berlin, den
Auftraggeber	Auftragnehmer Lamano GmbH & Co. KG Prenzlauer Allee 36G 10405 Berlin
Unterschrift	Unterschrift

Anlage 1

Darstellung der technischen und organisatorischen Sicherheitsmaßnahmen gemäß Art. 32 DSGVO

Vorwort

Das System LamaPoll ermöglicht die Erhebung, Verarbeitung und Nutzung personenbezogener Daten. Ob, wie und welche personenbezogenen Daten verarbeitet, erhoben und genutzt werden bestimmt stets der Auftraggeber.

Das System LamaPoll und alle dazugehörigen Datenserver sind bei der Strato-AG gehostet und verfügen über die BS-7799-TÜV-Zertifizierung sowie über die unabhängige TÜV-Zertifizierung nach DIN ISO 27001. Die Technischen und Organisatorischen Maßnahmen unseres Unterauftragnehmers werden daher mit aufgeführt.

Falls zum Zwecke der Fehlerbehebung, Wartung oder Weiterentwicklung der Software LamaPoll eine lokale (in unseren Büroräumen) Kopie erforderlich ist, wird diese zunächst anonymisiert (zum Beispiel E-Mali-Adressen von Teilnehmern werden gelöscht) und dann ausschließlich auf verschlüsselten Festplatten / Partitionen hinterlegt, wobei der Zugriff nur durch befugte, autorisierte, geschulte Mitarbeiter möglich ist.

Für die Verarbeitung der personenbezogenen Daten gelten folgend beschriebene technischen und organisatorischen Maßnahmen:

1. Vertraulichkeit

1.1. Zutrittskontrolle

Zutrittsbewilligung und Schlüsselübergabe erfolgt ausschließlich durch die Geschäftsleitung und wird schriftlich dokumentiert. Falls Betriebsfremde Zutritt zu den Büroräumen benötigen, werden diese durch einen LamaPoll-Mitarbeiter begleitet. Das Bürogebäude ist Videoüberwacht.

Für Subunternehmer STRATO AG gilt:

Unbefugten ist der Zutritt zu Räumen zu verwehren, in denen Datenverarbeitungsanlagen untergebracht sind.

- Festlegung von Sicherheitsbereichen
- Realisierung eines wirksamen Zutrittsschutzes
- Protokollierung des Zutritts
- Festlegung Zutrittsberechtigter Personen
- Verwaltung von personengebundenen Zutrittsberechtigungen
- Begleitung von Fremdpersonal
- Überwachung der Räume

1.2. Zugangskontrolle

Der Zugang zu Systemen erfolgt mit Authentifizierung durch individuelle Benutzerkennung und Passwort. Passwörter müssen unserer Passwortrichtlinie entsprechen (u.A. min. 8 Zeichen mit min. 3 Zeichengruppen). Zugangsberechtigungen werden ausschließlich durch die Geschäftsführung gewährt und schriftlich dokumentiert. Unsere Systeme sind vor unbefugtem Zugang durch Firewalls und Anti-

Viren-Software geschützt. Alle Arbeitsplätze (PC, Tablets, Testgeräte) werden bei Verlassen des Arbeitsplatzes passwortgeschützt.

Für Subunternehmer STRATO AG gilt:

Es ist zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden.

- Festlegung des Schutzbedarfs
- Zugangsschutz
- Umsetzung sicherer Zugangsverfahren, starke Authentisierung
- Umsetzung einfacher Authentisierung per Username Passwort
- Protokollierung des Zugangs
- Monitoring bei kritischen IT-Systemen
- Gesicherte (verschlüsselte) Übertragung von Authentisierungsgeheimnissen
- Sperrung bei Fehlversuchen/Inaktivität und Prozess zur Rücksetzung gesperrter Zugangskennungen
- Verbot Speicherfunktion für Passwörter und/oder Formulareingaben (Server/Clients)
- Festlegung befugter Personen
- Verwaltung und Dokumentation von personengebundenen Authentifizierungsmedien und
- Zugangsberechtigungen
- Automatische Zugangssperre und Manuelle Zugangssperre

1.3. Zugriffskontrolle

Der Zugriff auf unsere Systeme sowie auf das Befragungstool erfolgt mit Authentifizierung durch individuelle Benutzerkennung und Passwort. Passwörter müssen unserer Passwortrichtlinie entsprechen. LamaPoll ist mit einem Schutz vor Brute-Force-Angriffen gesichert. Server sind mit Firewall und Anti-Virensoftware gesichert. Zugriff auf Server ist nur durch autorisierte Mitarbeiter mittels individuellen RSA-Schlüsseln möglich. Protokollierung von Benutzeraktionen sowohl LamaPoll- als auch Serverseitig, regelmäßige Auswertung sowie Monitoring (elektronische Meldung bei Störung und Verdachtsfällen).

Mitarbeiter unseres Hosters (Strato-AG) haben auf dedizierte Root-Server keinen Zugriff.

Für Subunternehmer STRATO AG gilt:

Es kann nur auf die Daten zugegriffen, für die eine Zugriffsberechtigung besteht. Daten können bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden.

- Erstellen eines Berechtigungskonzepts
- Umsetzung von Zugriffsbeschränkungen
- Vergabe minimaler Berechtigungen
- Verwaltung und Dokumentation von personengebundenen Zugriffsberechtigungen
- Vermeidung der Konzentration von Funktionen.

1.4. Trennungskontrolle

Die Speicherung erfolgt für jeden Mandanten getrennt. Auftragsdaten (Befragungsergebnisse) und Vertragsdaten (Name, Anschrift usw. des Vertragspartners) sind ebenfalls getrennt voneinander gespeichert. Die Trennung wird durch Mandanten ID umgesetzt.

Für Subunternehmer STRATO AG gilt:

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

- Datensparsamkeit im Umgang mit personenbezogenen Daten
- Getrennte Verarbeitung verschiedener Datensätze

- Regelmäßige Verwendungszweckkontrolle und Löschung
- Trennung von Test- und Entwicklungsumgebung

2. Integrität

2.1. Weitergabekontrolle

Keine Weitergabe, Übermittlung, Übertragung oder Transport von personenbezogenen Daten durch unsere Mitarbeiter im System vorgesehen. Alle Mitarbeiter werden nach Artikel 28 EU DS-GVO zur Vertraulichkeit verpflichtet, unterliegen unserer Geheimhaltungsverpflichtung und werden regelmäßig im Umgang mit vertraulichen und personenbezogenen Daten geschult. Im Rahmen des Kundensupports exportierte Daten werden ausschließlich verschlüsselt (via SSL) übertragen, nicht gespeichert, sondern nach Betreuungsfall unwiederbringlich gelöscht. Der Export wird protokolliert.

Für Subunternehmer STRATO AG gilt:

Ziel der Weitergabekontrolle ist es, 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.

- Festlegung empfangs- /weitergabeberechtigter Instanzen/Personen
- Prüfung der Rechtmäßigkeit der Übermittlung ins Ausland
- Protokollierung von Übermittlungen gemäß Protokollierungskonzept
- Sichere Datenübertragung zwischen Server und Client
- Sicherung der Übertragung im Backend
- Sichere Übertragung zu externen Systemen
- Risikominimierung durch Netzseparierung
- Implementation von Sicherheitsgateways an den Netzübergabepunkten
- Härtung der Backendsysteme
- Beschreibung der Schnittstellen
- Umsetzung einer Maschine-Maschine-Authentisierung
- Sichere Ablage von Daten, inkl. Backups
- Gesicherte Speicherung auf mobilen Datenträgern
- Einführung eines Prozesses zur Datenträgerverwaltungen
- Prozess zur Sammlung und Entsorgung
- Datenschutzgerechter Lösch- und Zerstörungsverfahren
- Führung von Löschprotokollen

2.2. Eingabekontrolle

Alle Eingaben werden vom Auftraggeber selbst vorgenommen. Die Protokollierung der Benutzeraktionen ermöglicht Überprüfung, wer, wann und wie personenbezogene Daten eingegeben, verändert oder gelöscht hat.

Für Subunternehmer STRATO AG gilt:

Zweck der Eingabekontrolle ist es, zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

- Protokollierung der Eingaben
- Dokumentation der Eingabeberechtigungen

3. Verfügbarkeit und Belastbarkeit

3.1. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

Nahezu 100%-ige Verfügbarkeit durch autarke und redundante Stromversorgung, Kühlung und Internetanbindung. Alle Daten sind in einem RAID-1-Array gespeichert. Das bedeutet, dass alle Festplatten redundant und gespiegelt vorhanden sind. Bei Ausfall einer Festplatte springt automatisch und ohne Unterbrechung unseres Dienstes eine Ersatzfestplatte ein. LamaPoll wird grundsätzlich ohne Unterbrechung angeboten.

Alle Daten werden täglich gesichert. Die Sicherung erfolgt verschlüsselt (AES-256) auf 3 physisch getrennten Speichermedien. Somit ist ein optimaler Schutz vor Datenverlust gewährleistet.

Unsere Programmierer befolgen einen Katalog von Codierungsrichtlinien, welche eine sichere und stabile Programmierung von LamaPoll gewährleisten und vor Datenmanipulation und -verlust schützen.

Betriebssysteme und verwendete Anwendungen werden stets aktualisiert und verwenden immer die neusten Patches.

Für Subunternehmer STRATO AG gilt:

- Brandschutz
- Redundanz der Primärtechnik
- Redundanz der Stromversorgung
- Redundanz der Kommunikationsverbindungen
- Monitoring
- Resourcenplanung und Bereitstellung
- Abwehr von systembelastendem Missbrauch
- Datensicherungskonzepte und Umsetzung
- Regelmäßige Prüfung der Notfalleinrichtungen

3.2. Wiederherstellbarkeit

Der Auftragnehmer gewährleistet die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu diesen bei einem physischen oder technischen Zwischenfall durch die folgenden Maßnahmen rasch wiederherzustellen:

Dokumentiertes Backup-Verfahren und regelmäßige Sicherungskopien sind vorhanden. Die Backups erfolgen täglich, sind verschlüsselt, werden physisch und räumlich getrennt vom System gesichert. Zustand und Prozess unterliegen regelmäßiger Kontrolle. Es gibt erprobte Prozesse zur Einspielung der Backups (Rücksicherung).

Die Ergebnisse von Umfragen werden parallel auf mehrere (>2) Server gespeichert und synchronisiert, bei Zwischenfällen springt ein Ersatzserver ein.

Für Subunternehmer STRATO AG gilt:

- Notfallplan
- Datensicherungskonzepte und Umsetzung

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

4.1. Auftragskontrolle (Art. 32 Abs. 3 und 4 DSGVO)

Die Protokollierung der Benutzeraktionen garantiert die Verarbeitung gemäß Weisungen des Auftraggebers. Der Auftragsverarbeitungsvertrag nach Artikel 28 EU DS-GVO spezifiziert die Rechte und Pflichten von Auftraggeber (Kunde) und Auftragnehmer (LamaPoll).

Alle Mitarbeiter sind im Umgang mit personenbezogenen Daten geschult.

Für die Auftragskontrolle der Serverräume:

Unsere Mitarbeiter kennen den Datenverarbeitungszweck. Sie erhalten schriftliche Weisung zum Umgang mit personenbezogenen Daten.

Ein IT-Organisationshandbuch / IT-Sicherheitskonzept ist vorhanden. Unterauftragsverhältnisse werden schriftlich beauftragt.

Für Subunternehmer STRATO AG gilt:

Ziel der Auftragskontrolle ist es, zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

- Auswahl weiterer Auftragnehmer nach geeigneten Garantien
- Abschluss einer Vereinbarung zur Auftragsverarbeitung mit weiteren Auftragnehmern
- Abschluss einer Vereinbarung zur Auftragsverarbeitung mit STRATO

4.2. Datenschutzmanagement

Der Auftragnehmer gewährleistet einen Prozess zur regelmäßigen Überprüfung und Bewertung der Wirksamkeit der technischen und organisatorischen Schutzmaßnahmen. Dies geschieht durch:

- Es wurde ein Datenschutzbeauftragter schriftlich bestellt.
- Alle Mitarbeiter wurden schriftlich auf die Einhaltung datenschutzrechtlicher Vorschriften gem. Art. 5 DSGVO verpflichtet und unterwiesen.
- Die mit der Datenverarbeitung betrauten Mitarbeiter wurden auf ihre Pflicht zur Verschwiegenheit über Betriebs- und Geschäftsgeheimnisse hingewiesen.
- Die mit der Datenverarbeitung betrauten Mitarbeiter wurden in Datenschutzschulungen mit den Vorschriften des Bundesdatenschutzgesetzes und anderer Vorschriften über den Datenschutz gemäß Art. 39 DSGVO vertraut gemacht.
- Wenn aus organisatorischen Gründen Funktionsüberschneidungen bestehen, wird das Vier-Augen-Prinzip angewendet und dokumentiert.
- Es existiert eine definierte Vertreterregelung innerhalb von Funktionsgruppen.

Für Subunternehmer STRATO AG gilt:

- Festlegung von Verantwortlichkeiten
- Umsetzung und Kontrolle geeigneter Prozesse
- Melde- und Freigabeprozess
- Umsetzung von Schulungsmaßnahmen
- Verpflichtung auf Vertraulichkeit
- Regelungen zur internen Aufgabenverteilung
- Beachtung von Funktionstrennung und –zuordnung
- Einführung einer geeigneten Vertreterregelung