

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

zwischen Ihnen als Verantwortlicher eines beantragten bzw. bereits bestehenden Verwaltungszuganges zu unserer Umfrage-Plattform LamaPoll, entsprechend unseren Allgemeinen Geschäftsbedingungen (AGB)

.....
.....
.....

(hier nachfolgend als „Auftraggeber“ bezeichnet)

und uns,

der Lamano GmbH & Co. KG
Prenzlauer Allee 36 G
10405 Berlin

- Betreiber des Online-Umfragedienstes „LamaPoll“ unter www.lamapoll.de -

als Auftragsverarbeiter

(hier im Folgenden als „Auftragnehmer“ bezeichnet)

Präambel

Der Auftragnehmer soll entsprechend eines gesondert erteilten Auftrags für den Auftraggeber die hier in § 2 nochmals klarstellend und zusammengefasst näher genannten Leistungen erbringen. Wesentlicher Teil dieses gesondert erteilten Auftrags ist dabei die Verarbeitung von im Regelfall auch personenbezogenen Daten für den Auftraggeber. Insbesondere Art. 28 DS-GVO stellt bestimmte Anforderungen an eine solche Auftragsverarbeitung. Zur Wahrung dieser Anforderungen schließen die Parteien die nachfolgende Vereinbarung, die für sämtliche Tätigkeiten des Auftragnehmers für den Auftraggeber im Zusammenhang mit dem gesondert erteilten Auftrag gilt.

§ 1 Begriffsbestimmung

(1) Verantwortlicher ist gem. Art. 4 Abs. 7 DS-GVO die Stelle, die allein oder gemeinsam mit anderen Verantwortlichen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.

(2) Auftragsverarbeiter ist gem. Art. 4 Abs. 8 DS-GVO eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.

(3) Personenbezogene Daten sind gem. Art. 4 Abs. 1 DS-GVO alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann.

(4) Besonders schutzbedürftige personenbezogene Daten sind personenbezogenen Daten gem. Art. 9 DS-GVO, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit von Betroffenen hervorgehen, personenbezogene Daten gem. Art. 10 DS-GVO über strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmaßnahmen sowie genetische Daten gem. Art. 4 Abs. 13 DS-GVO, biometrischen Daten gem. Art. 4 Abs. 14 DS-GVO, Gesundheitsdaten gem. Art. 4 Abs. 15 DS-GVO sowie Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person.

(5) Verarbeitung ist gem. Art. 4 Abs. 2 DS-GVO jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte 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.

(6) Aufsichtsbehörde ist gem. Art. 4 Abs. 21 DS-GVO eine von einem Mitgliedstaat gem. Art. 51 DS-GVO eingerichtete unabhängige staatliche Stelle.

§ 2 Vertragsgegenstand des Hauptvertrages; Umfang, Zweck und Art der Verarbeitung personenbezogener Daten

(1) Der Auftragnehmer stellt dem Auftraggeber entsprechend eines gesonderten Auftrags und unter Beachtung und Einbeziehung seiner AGB seine Online-Plattform (mitunter hier auch „Umfrage-

Plattform“ genannt) technisch zur Verfügung, mit derer der Auftraggeber unter Nutzung der technischen Infrastruktur des Auftragnehmers (hardware- wie auch softwareseitig) zur Planung, Durchführung und auch Auswertung von eigenen Online-Umfragen im Stande ist (Hauptvertrag). Dabei unterliegen jene Umfragen des Auftraggebers, die er mittels der Infrastruktur des Auftragnehmers tatsächlich plant, durchführt und auswertet, der alleinigen rechtlichen Verantwortung des Auftraggebers (beispielsweise auch mit Blick auf die rechtliche Zulässigkeit zu stellender Fragen, von ihm selbst fest vorgegebener Antwortmöglichkeiten, der Einbeziehung von Personen zum Zwecke der Teilnahme an Umfragen sowie auch beispielsweise hinsichtlich der Auswertung und Verwendung etwaiger erhaltener Antworten). Die gesamte tatsächliche Nutzung der Umfrage-Infrastruktur des Auftragnehmers durch den Auftraggeber entsprechend des Hauptvertrages unterliegt allein den durch bloße technische Konfiguration vorgenommenen Vorgaben des Auftraggebers und somit auch allein dessen rechtlicher Bewertung und rechtlicher Verantwortung hinsichtlich der Zulässigkeit seiner Umfragen. Nach alledem ist der Auftraggeber in der Planung, Festlegung, Veröffentlichung, Durchführung und Auswertung seiner Umfragen in gänzlich eigener Verantwortung frei. Er ist somit auf faktischer Ebene - ungeachtet der Rechtslage im Einzelfall - allein durch technisch womöglich im Einzelfall vorgegebene Umstände begrenzt und aus diesem Grunde auch gänzlich allein für seine Umfragen mittels der Infrastruktur des Auftragnehmers in jeglicher Hinsicht und insbesondere auch rechtlich verantwortlich. Im Zuge dieser technischen, auftragsgemäßen Bereitstellung der Online-Plattform des Auftragnehmers, erhält der Auftragnehmer, als technischer Betreiber der Umfrage-Plattform, naturgemäß ebenfalls potentiell Zugriff auf etwaige hierbei anfallende und womöglich auch personenbezogene Daten bzw. Kontakt mit jenen. Der Auftragnehmer verarbeitet diese jedoch ausschließlich im Auftrag und allein nach Weisung des Auftraggebers.

(2) Mit Blick auf den Umfang der Datenverarbeitungen kommen je nach konkreter Verwendung der Online-Plattform des Auftragnehmers durch den Auftraggeber im Einzelfall (Weisung) grundsätzlich sämtliche mit und/oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgänge und/oder Vorgangsreihen im Zusammenhang mit personenbezogenen Daten wie insbesondere 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 andere Formen der Bereitstellung, der Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung durch den Auftragnehmer für den Auftraggeber in Betracht.

(3) Zweck dieser Datenverarbeitungen durch den Auftragnehmer für den Auftraggeber ist es, dem Auftraggeber die Konzeption, Verwaltung, Durchführung und Auswertung von technisch beliebigen Online-Umfragen zu ermöglichen, wobei die konkreten Umfrage-Inhalte, Umfrage-Teilnehmer, Umfrage-Auswertungen usw. allein von dem Auftraggeber verantwortet und durch entsprechende Konfiguration und Planung vorgegeben werden.

(4) Allein dem Auftraggeber obliegt die Beurteilung und Sicherstellung der Zulässigkeit der Datenverarbeitung.

(5) Zur Konkretisierung der beiderseitigen datenschutzrechtlichen Rechte und Pflichten schließen die Parteien diese vorliegende Vereinbarung. Die den Datenschutz betreffenden Regelungen der vorliegenden Vereinbarung gehen im Zweifel den Regelungen des Hauptvertrags vor.

(6) Die Bestimmungen dieses Vertrages finden Anwendung auf alle Tätigkeiten, die mit dem Hauptvertrag in Zusammenhang stehen und bei der der Auftragnehmer und seine Beschäftigten und/oder durch den Auftragnehmer Beauftragte mit personenbezogenen Daten in Berührung kommen, die vom Auftraggeber stammen oder für den Auftraggeber oder durch den Auftraggeber erhoben wurden.

(7) Die Laufzeit dieses Vertrags richtet sich nach der Laufzeit des Hauptvertrages, sofern sich aus den nachfolgenden Bestimmungen nicht darüberhinausgehende Verpflichtungen oder Kündigungsrechte ergeben.

§ 3 Weisungen

(1) Der Auftragnehmer darf Daten nur im Rahmen des Hauptvertrags und gemäß den Weisungen des Auftraggebers erheben, verarbeiten oder nutzen; dies gilt insbesondere auch in Bezug auf die Übermittlung personenbezogener Daten in ein Drittland oder an eine internationale Organisation. Wird der Auftragnehmer durch das Recht der Europäischen Union oder der Mitgliedstaaten, dem er unterliegt, zu weiteren Verarbeitungen verpflichtet, teilt er dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

(2) Die Weisungen des Auftraggebers werden insbesondere elektronisch über den hierzu dem Auftraggeber passwortgeschützt bereitgestellten Verwaltungsbereich zur Bedienung der Online-Plattform des Auftragnehmers („Backend“) vom Auftraggeber in der Weise an den Auftragnehmer erteilt, ergänzt, geändert oder ersetzt, dass dieser dort im Einzelnen durch seine softwareseitigen Einstellungen über seinen Verwaltungszugang vorgibt, wie Online-Umfragen für den Auftraggeber konzeptioniert, gespeichert, durchgeführt, ausgewertet und auch wieder beendet und letztlich gelöscht werden sollen. Zudem kann der Auftraggeber auch in schriftlicher Form und auch in Textform einzelne Weisungen erteilen, ergänzen, ändern oder ersetzen. Der Auftraggeber ist jederzeit zur Erteilung entsprechender Weisungen berechtigt. Dies umfasst auch Weisungen in Hinblick auf die Berichtigung, Löschung und Sperrung von Daten.

(3) Soweit der Auftraggeber Personen zum Online-System des Auftragnehmers weitere Verwaltungszugänge (Legitimation über Benutzername und Passwort) einrichtet, so benennt er diese dem Auftragnehmer gegenüber damit insoweit als ebenfalls datenschutzrechtlich für den Auftraggeber Weisungsberechtigte im Sinne dieser Vereinbarung.

(4) Alle erteilten Weisungen sind sowohl vom Auftraggeber als auch vom Auftragnehmer zu dokumentieren. Weisungen, die über die hauptvertraglich vereinbarte Leistung hinausgehen, werden als Antrag auf Leistungsänderung behandelt.

(5) Ist der Auftragnehmer der Ansicht, dass eine Weisung des Auftraggebers gegen datenschutzrechtliche Bestimmungen verstößt, hat er den Auftraggeber unverzüglich darauf hinzuweisen. Der Auftragnehmer ist berechtigt, die Durchführung der betreffenden Weisung solange auszusetzen, bis diese durch den Auftraggeber bestätigt oder geändert wird. Der Auftragnehmer darf die Durchführung offensichtlich rechtswidriger, auch mit Blick auf den Hauptvertrag vertragsrechtswidriger Weisungen ablehnen.

§ 4 Besondere Informationspflichten des Auftraggebers

(1) Aus der Funktionsweise der Umfrage-Plattform des Auftraggebers, aus dem zugrundeliegenden Hauptvertrag zwischen Auftraggeber und Auftragnehmer und auch aus den §§ 2 und 3 dieser Vereinbarung ergibt sich, dass allein der Auftraggeber für das Ob und Wie seiner Umfragen selbst verantwortlich ist. Aus diesem Grund ist es die Pflicht des Auftraggebers, unbedingt dafür Sorge zu tragen, dass bei sämtlichen Datenverarbeitungen, die der Auftraggeber mittels der Infrastruktur des Auftragnehmers durchführt bzw. im Auftrag des Auftraggebers durch den Auftragnehmer durchführen lässt, sämtliche von diesen Datenverarbeitungen Betroffenen entsprechend der gesetzlichen Vorgaben umfassend und zutreffend informiert werden. Dies betrifft beispielsweise also Informationspflichten gegenüber Betroffenen nach Art. 13 und 14 DS-GVO, die aufgrund der Funktionsweise der Umfrage-Plattform der Auftraggeber zu erfüllen hat, soweit er die Umfrage-Plattform des Auftragnehmers nutzt.

(2) Der Auftragnehmer stellt dem Auftraggeber zu diesem Zwecke technische Möglichkeiten zur Verfügung, die es dem Auftraggeber ermöglichen, seinen Informationspflichten insoweit

nachzukommen, als dass der Auftraggeber (auch) datenschutzrechtliche Hinweise zur Erfüllung seiner Informationspflichten inhaltlich einstellen und deren Anzeige so konfigurieren kann, dass diese – beispielsweise bei der Durchführung von Umfragen – stets prominent und für den Betroffenen gut sichtbar eingesehen werden können.

(3) Um eine vollständige und korrekte Erstellung der datenschutzrechtlichen Hinweise an Betroffene durch den Auftraggeber inhaltlich zu ermöglichen, stellt der Auftragnehmer dem Auftraggeber auch stets aktuelle „Ergänzende Hinweise für den Auftraggeber zu den technisch ihm im Einzelnen möglichen Datenverarbeitungsvorgängen mittels der Online-Plattform des Auftragnehmers“ in seinem Verwaltungszugang zur Verfügung, die es dem Auftraggeber ermöglichen, sämtliche Informationen zu erhalten, die für den Auftraggeber relevant sind, um Betroffene vollständig und zutreffend zur Erfüllung der datenschutzrechtlichen Vorgaben informieren zu können (beispielsweise etwa hinsichtlich der Speicherdauer spezifischer Daten).

(4) Für den Fall, dass der Auftraggeber im Einzelfall über die in Abs. 3 benannten und online für den Auftraggeber stets verfügbaren Hinweise unerwarteter Weise noch hinausgehende Informationen benötigt, um seine Hinweispflichten erfüllen zu können, nimmt er hierzu umgehend Kontakt mit dem Auftragnehmer auf, der ihm alle etwaigen weiteren, nötigen Informationen hierzu zukommen lässt.

(5) Der Auftraggeber ist verpflichtet, inhaltlich zutreffende, vollständige und rechtskonforme Datenschutzhinweise betreffend die Nutzung der Umfrage-Plattform des Auftragnehmers zu erstellen und diese zur Verwendung zu hinterlegen, bevor er die Umfrage-Plattform des Auftragnehmers nutzt bzw. diese in seinem Auftrag durch den Auftragnehmer nutzen lässt.

(6) Der Auftraggeber ist für die Rechtmäßigkeit der Verarbeitung der Daten seiner Umfragen sowie für die Wahrung der Rechte der Betroffenen auch im Verhältnis der Parteien zueinander allein verantwortlich.

§ 5 Art der verarbeiteten Daten, Kreis der Betroffenen

(1) Mit Blick auf die Art der für den Auftraggeber verarbeiteten Daten kommen je nach konkreter Verwendung der Online-Plattform des Auftragnehmers nach Wahl des Auftraggebers im Einzelfall (Weisung) grundsätzlich sämtliche denkbaren Arten und Kategorien personenbezogener Daten in Betracht; insbesondere (aber nicht ausschließlich) beispielsweise auch „besondere Kategorien“ personenbezogener Daten gem. Art. 9 DS-GVO, personenbezogene Daten gem. Art. 10 DS-GVO und/oder womöglich auch Daten, die einer besonderen berufsrechtlichen Verschwiegenheitsverpflichtung im Sinne von § 203 StGB aus weiteren Rechtsnormen unterliegen.

(2) Ebenso unterliegen auch die Kategorien betroffener Personen der uneingeschränkten und alleinigen Disposition des Auftraggebers, sodass insbesondere (aber nicht ausschließlich) Beschäftigte, Interessenten, Lieferanten, Kunden, Patienten, Mandanten, Besucher und/oder Antragsteller als betroffene Personen nach Wahl des Auftraggebers in Betracht kommen können.

§ 6 Schutzmaßnahmen des Auftragnehmers

(1) Der Auftragnehmer ist verpflichtet, die gesetzlichen Bestimmungen über den Datenschutz zu beachten und die aus dem Bereich des Auftraggebers erlangten Informationen nicht an Dritte weiterzugeben oder deren Zugriff auszusetzen. Unterlagen und Daten sind gegen die Kenntnisnahme durch Unbefugte unter Berücksichtigung des Stands der Technik zu sichern.

(2) Der Auftragnehmer wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er trifft alle

erforderlichen technischen und organisatorischen Maßnahmen zum angemessenen Schutz der Daten des Auftraggebers gem. Art. 32 DSGVO, insbesondere mindestens die in Anlage 1 aufgeführten Maßnahmen der

- Zutrittskontrolle
- Zugangskontrolle
- Zugriffskontrolle
- Weitergabekontrolle
- Eingabekontrolle
- Auftragskontrolle
- Verfügbarkeitskontrolle
- Trennungskontrolle

Eine Änderung der getroffenen Sicherheitsmaßnahmen bleibt dem Auftragnehmer vorbehalten, wobei er sicherstellt, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird.

(3) Den bei der Datenverarbeitung durch den Auftragnehmer beschäftigten Personen ist es untersagt, personenbezogene Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen. Der Auftragnehmer wird alle Personen, die von ihm mit der Bearbeitung und der Erfüllung dieses Vertrages betraut werden (im folgenden Mitarbeiter genannt), entsprechend verpflichten (Verpflichtung zur Vertraulichkeit, Art. 28 Abs. 3 lit. b DS-GVO) und mit der gebotenen Sorgfalt die Einhaltung dieser Verpflichtung sicherstellen. Diese Verpflichtungen müssen so gefasst sein, dass sie auch nach Beendigung dieses Vertrages oder des Beschäftigungsverhältnisses zwischen dem Mitarbeiter und dem Auftragnehmer bestehen bleiben. Dem Auftraggeber sind die Verpflichtungen auf Verlangen in geeigneter Weise nachzuweisen.

§ 7 Rechte und Pflichten des Auftraggebers

(1) Bei Störungen, Verdacht auf Datenschutzverletzungen oder Verletzungen vertraglicher Verpflichtungen des Auftragnehmers, Verdacht auf sicherheitsrelevante Vorfälle oder andere Unregelmäßigkeiten bei der Verarbeitung der personenbezogenen Daten durch den Auftragnehmer, bei ihm im Rahmen des Auftrags beschäftigten Personen oder durch Dritte wird der Auftragnehmer den Auftraggeber unverzüglich in Schriftform oder Textform informieren. Die Meldung über eine Verletzung des Schutzes personenbezogener Daten enthält zumindest folgende Informationen:

- a) eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der Zahl der betroffenen Personen, der betroffenen Kategorien und der Zahl der betroffenen personenbezogenen Datensätze;
- b) eine Beschreibung der von dem Auftragnehmer ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

(2) Der Auftragnehmer trifft unverzüglich die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der Betroffenen, informiert hierüber den Auftraggeber und ersucht um weitere Weisungen.

(3) Der Auftragnehmer ist darüber hinaus verpflichtet, dem Auftraggeber jederzeit Auskünfte zu erteilen, soweit dessen Daten von einer Verletzung nach Absatz 1 betroffen sind.

(4) Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren, sofern ihm dies nicht durch gerichtliche oder behördliche Anordnung untersagt ist. Der Auftragnehmer wird in diesem Zusammenhang alle zuständigen Stellen unverzüglich darüber informieren, dass die Entscheidungshoheit über die Daten ausschließlich beim Auftraggeber als „Verantwortlicher“ im Sinne der DS-DVO liegt.

(5) Über wesentliche Änderungen der Sicherheitsmaßnahmen nach § 6 Abs. 2 hat der Auftragnehmer den Auftraggeber unverzüglich zu unterrichten.

(6) Der Auftragnehmer und gegebenenfalls sein Vertreter führen ein Verzeichnis zu allen Kategorien von im Auftrag des Auftraggebers durchgeführten Tätigkeiten der Verarbeitung, das alle Angaben gem. Art. 30 Abs. 2 DS-GVO enthält.

(7) An der Erstellung des Verfahrensverzeichnisses durch den Auftraggeber hat der Auftragnehmer im angemessenen Umfang mitzuwirken. Er hat dem Auftraggeber die jeweils erforderlichen Angaben in geeigneter Weise mitzuteilen.

§ 8 Kontrollrechte des Auftraggebers

1) Der Auftraggeber überzeugt sich selbst vor der Aufnahme der Datenverarbeitung und sodann im Anschluss regelmäßig von den technischen und organisatorischen Maßnahmen des Auftragnehmers. Hierfür kann er zum Beispiel Auskünfte des Auftragnehmers einholen, sich vorhandene Testate von Sachverständigen, Zertifizierungen oder internen Prüfungen vorlegen lassen oder die technischen und organisatorischen Maßnahmen des Auftragnehmers nach rechtzeitiger Abstimmung zu den üblichen Geschäftszeiten selbst persönlich prüfen bzw. durch einen sachkundigen Dritten prüfen lassen, sofern dieser nicht in einem Wettbewerbsverhältnis zum Auftragnehmer steht. Der Auftraggeber wird Kontrollen nur im erforderlichen Umfang und im Rahmen des Zumutbaren durchführen und die Betriebsabläufe des Auftragnehmers dabei nicht unverhältnismäßig stören. Eine persönliche Prüfung bzw. Prüfung durch Dritte kann der Auftragnehmer von der Unterzeichnung einer hinreichend vertragsstrafenbewehrten Verschwiegenheitsvereinbarung hinsichtlich der Daten anderer Kunden und der eingerichteten technischen und organisatorischen Maßnahmen abhängig machen. Sollte der durch den Auftraggeber beauftragte Prüfer in einem Wettbewerbsverhältnis zu dem Auftragnehmer stehen, hat der Auftragnehmer gegen diesen ein Einspruchsrecht. Sollte eine Datenschutzaufsichtsbehörde oder eine sonstige hoheitliche Aufsichtsbehörde des Auftraggebers eine Prüfung vornehmen, ist die Unterzeichnung einer Verschwiegenheitsverpflichtung dann nicht erforderlich, wenn diese Aufsichtsbehörde einer berufsrechtlichen oder gesetzlichen Verschwiegenheit unterliegt, bei der ein Verstoß nach dem Strafgesetzbuch strafbewehrt ist.

(2) Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf dessen Anforderung hin innerhalb einer angemessenen Frist alle Auskünfte und Nachweise zur Verfügung zu stellen, die zur Durchführung einer Kontrolle der technischen und organisatorischen Maßnahmen des Auftragnehmers erforderlich sind. Für die gesamte Unterstützung hinsichtlich der Durchführung einer Inspektion durch den Auftraggeber, durch einen Dritten des Auftraggebers oder aber auch durch eine Aufsichtsbehörde des Auftraggebers darf der Auftragnehmer eine Vergütung vom Auftraggeber verlangen, wenn und ggf. wie dies im Hauptvertrag im Einzelnen vereinbart ist.

(3) Der Auftragnehmer ist jedoch berechtigt, nach eigenem Ermessen und unter pflichtgemäßer Berücksichtigung sämtlicher gesetzlichen Verpflichtungen Informationen nicht zu offenbaren, die sensibel im Hinblick auf die Geschäfte des Auftragnehmers sind oder wenn der Auftragnehmer durch

deren Offenbarung gegen gesetzliche oder andere vertragliche Regelungen verstoßen würde, sofern diese nicht den rechtsmissbräuchlichen Zweck haben, die Rechte des Auftraggebers einzuschränken. Der Auftraggeber ist nicht berechtigt, Zugang zu Daten oder Informationen über andere Kunden des Auftragnehmers, zu Informationen hinsichtlich Kosten, zu Qualitätsprüfungs- und Vertragsmanagementberichten sowie zu sämtlichen anderen vertraulichen Daten des Auftragnehmers, die nicht unmittelbar relevant für die Überprüfungszwecke sind, zu erhalten.

(4) Der Auftraggeber dokumentiert das Kontrollergebnis und teilt es dem Auftragnehmer umgehend und vollständig mit. Bei Fehlern oder Unregelmäßigkeiten, die der Auftraggeber insbesondere bei der Prüfung von Auftragsergebnissen feststellt, hat er den Auftragnehmer unverzüglich zu informieren. Werden bei der Inspektion Sachverhalte festgestellt, deren zukünftige Vermeidung Änderungen des angeordneten Verfahrensablaufs erfordern, teilt der Auftraggeber dem Auftragnehmer die notwendigen Verfahrensänderungen unverzüglich mit.

(5) Der Auftragnehmer stellt dem Auftraggeber auf dessen Wunsch ein umfassendes und aktuelles Datenschutz- und Sicherheitskonzept für die Auftragsverarbeitung sowie über die zugriffsberechtigten Personen zur Verfügung.

(6) Der Auftragnehmer weist dem Auftraggeber die Verpflichtung der Mitarbeiter nach § 6 Abs. 4 auf Verlangen nach.

§ 9 Einsatz von Subunternehmern

(1) Die vertraglich vereinbarten Leistungen werden unter Einschaltung der STRATO AG, Pascalstraße 10 in 10587 Berlin als Subunternehmer für das Serverhosting durchgeführt. Der Auftragnehmer ist im Rahmen seiner vertraglichen Verpflichtungen zur Begründung von weiteren Unterauftragsverhältnissen mit Subunternehmern („Subunternehmerverhältnis“) befugt. Er setzt den Auftraggeber hiervon unverzüglich in Kenntnis. Der Auftragnehmer ist verpflichtet, Subunternehmer sorgfältig nach deren Eignung und Zuverlässigkeit auszuwählen. Der Auftragnehmer hat bei der Einschaltung von Subunternehmern diese entsprechend den Regelungen dieser Vereinbarung zu verpflichten und dabei sicherzustellen, dass der Auftraggeber seine Rechte aus dieser Vereinbarung (insbesondere seine Prüf- und Kontrollrechte) auch direkt gegenüber den Subunternehmern wahrnehmen kann. Sofern eine Einbeziehung von Subunternehmern in einem Drittland erfolgen soll, hat der Auftragnehmer sicherzustellen, dass beim jeweiligen Subunternehmer ein angemessenes Datenschutzniveau gewährleistet ist (z.B. durch Abschluss einer Vereinbarung auf Basis der EU-Standarddatenschutzklauseln). Der Auftragnehmer wird dem Auftraggeber auf Verlangen den Abschluss der vorgenannten Vereinbarungen mit seinen Subunternehmern nachweisen.

(2) Ein Subunternehmerverhältnis im Sinne dieser Bestimmungen liegt nicht vor, wenn der Auftragnehmer Dritte mit Dienstleistungen beauftragt, die als reine Nebenleistungen anzusehen sind. Dazu gehören z. B. Post-, Transport- und Versandleistungen, Reinigungsleistungen, Telekommunikationsleistungen ohne konkreten Bezug zu Leistungen, die der Auftragnehmer für den Auftraggeber erbringt und Bewachungsdienste. Wartungs- und Prüfleistungen stellen zustimmungspflichtige Subunternehmerverhältnisse dar, soweit diese für IT-Systeme erbracht werden, die auch im Zusammenhang mit der Erbringung von Leistungen für den Auftraggeber genutzt werden.

§ 10 Anfragen und Rechte Betroffener

(1) Der Auftragnehmer unterstützt den Auftraggeber nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung von dessen Pflichten nach Art. 12–22 sowie 32 und 36 DS-GVO.

(2) Macht ein Betroffener Rechte, etwa auf Auskunftserteilung, Berichtigung oder Löschung hinsichtlich seiner Daten, unmittelbar gegenüber dem Auftragnehmer geltend, so reagiert dieser nicht selbstständig, sondern verweist den Betroffenen unverzüglich an den Auftraggeber und wartet dessen Weisungen ab.

(3) Für dahingehende Leistungen und etwaige Folgeleistungen nach dahingehenden Weisungen des Auftraggebers kann der Auftragnehmer vom Auftraggeber eine angemessene Vergütung nach den gesetzlichen Regelungen verlangen, sofern und soweit dem Auftragnehmer kein Fehlverhalten vorzuhalten ist, das Anlass jener Leistungen ist.

(4) Der Auftragnehmer wird dem Auftraggeber Informationen über die für den Auftraggeber gespeicherten Daten, die Empfänger jener Daten, an die der Auftragnehmer diese Informationen auftragsgemäß weitergibt, und auch den Zweck der Speicherung mitteilen, sofern dem Auftraggeber diese Informationen nicht selbst vorliegen oder er sie sich selbst beschaffen kann.

§ 11 Haftung; Freistellung

(1) Für die Haftung des Auftragnehmers nach diesem Vertrag gelten die Haftungsausschlüsse und -begrenzungen gemäß der AGB des Auftragnehmers.

(2) Soweit Dritte Ansprüche gegen den Auftragnehmer geltend machen, die ihre Ursache in einem schuldhaften Verstoß des Auftraggebers gegen diesen Vertrag oder gegen eine seiner Pflichten als datenschutzrechtlich Verantwortlicher haben, stellt der Auftraggeber den Auftragnehmer von diesen Ansprüchen auf erstes Anfordern frei.

(3) Der Auftraggeber verpflichtet sich, den Auftragnehmer auch von allen etwaigen Geldbußen, die gegen den Auftragnehmer verhängt werden, in dem Umfang auf erstes Anfordern freizustellen, in dem der Auftraggeber Anteil an der Verantwortung für den durch die Geldbuße sanktionierten Verstoß trägt.

§ 12 Außerordentliches Kündigungsrecht

Die Parteien können den Hauptvertrag fristlos beispielsweise auch dann kündigen, wenn eine Vertragspartei ihren Pflichten aus diesem Vertrag nicht nachkommt oder gesetzliche Datenschutzbestimmungen vorsätzlich oder grob fahrlässig verletzt. Bei einfachen - also weder vorsätzlichen noch grob fahrlässigen - Verstößen wird zunächst eine angemessene Frist gesetzt, innerhalb welcher der vorgeworfene Verstoß abgestellt werden kann.

§ 13 Laufzeit des Vertrages; Beendigung des Hauptvertrags; Datenlöschung

(1) Die Laufzeit und Kündigung dieses Vertrages richtet sich nach den Bestimmungen zur Laufzeit und Kündigung des Vertrages über die Nutzung des so genannten Verwaltungszugangs entsprechend des Hauptvertrages. Eine Kündigung des Verwaltungszugangs entsprechend des Hauptvertrages bewirkt

automatisch auch eine Kündigung dieses Vertrages. Eine isolierte Kündigung dieses Vertrages ist ausgeschlossen. Möglich bleibt jedoch eine einvernehmliche Aufhebung dieses Vertrages; beispielsweise zum Zwecke und im Rahmen eines späteren Abschlusses einer womöglich überarbeiteten Fassung dieses Vertrages.

(2) Der Auftragnehmer wird dem Auftraggeber nach Beendigung des gesamten Hauptvertrags oder jederzeit auf dessen Anforderung alle ihm überlassenen Unterlagen, Daten und Datenträger zurückgeben oder auf Wunsch des Auftraggebers löschen, sofern nicht eine gesetzliche Verpflichtung des Auftragnehmers zur weiteren Speicherung der Daten zum Auftrag des Auftraggebers besteht. Dies betrifft auch etwaige Datensicherungen beim Auftragnehmer. Der Auftragnehmer hat den dokumentierten Nachweis der ordnungsgemäßen Löschung noch vorhandener Daten zu führen.

(3) Der Auftraggeber hat das Recht, die vollständige und vertragsgerechte Rückgabe bzw. Löschung der Daten beim Auftragnehmer in geeigneter Weise zu kontrollieren.

(4) Der Auftragnehmer ist verpflichtet, auch über das Ende des Hauptvertrags hinaus die ihm im Zusammenhang mit dem Hauptvertrag bekannt gewordenen Daten vertraulich zu behandeln. Die vorliegende Vereinbarung bleibt über das Ende des Hauptvertrags hinaus solange gültig, wie der Auftragnehmer über personenbezogene Daten verfügt, die ihm vom Auftraggeber zugeleitet wurden oder die er für diesen erhoben hat.

(5) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Verarbeitung der Daten mit Bezug zum Auftrag des Auftraggebers dienen, dürfen durch den Auftragnehmer auch nach Vertragsende aufbewahrt werden.

§ 14 Schlussbestimmung

(1) Änderungen und Ergänzungen dieser Vereinbarung bedürfen der Textform. Dies gilt auch für die Aufhebung dieses Textformerfordernisses. Der Vorrang individueller Vertragsabreden bleibt hiervon unberührt.

(2) Es gilt das Recht der Bundesrepublik Deutschland unter Ausschluss des UN-Kaufrechts. Zwingende Bestimmungen des Staates, in dem Sie Ihren gewöhnlichen Aufenthalt haben, bleiben unberührt.

(3) Ausschließlicher Gerichtsstand ist bei Verträgen zwischen uns und Kaufleuten, juristischen Personen des öffentlichen Rechts oder öffentlich-rechtlichen Sondervermögen das für unseren Geschäftssitz zuständige Gericht in Berlin.

Anlagen: - Anlage 1 Darstellung der technischen und organisatorischen Sicherheitsmaßnahmen

Diese Vereinbarung wurde zwischen Auftraggeber und Auftragnehmer erfolgreich am (...) in elektronischer Weise abgeschlossen. / Diese Vereinbarung kann elektronisch mit dem Auftragnehmer geschlossen werden.

1. 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 36 G 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 Passworrichtlinie 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 Benutzererkennung 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 neuesten Patches.

Für Subunternehmer STRATO AG gilt:

- Brandschutz
- Redundanz der Primärtechnik
- Redundanz der Stromversorgung
- Redundanz der Kommunikationsverbindungen
- Monitoring
- Ressourcenplanung 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 Datenschutzs Schulungen 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