Vereinbarung zur Auftragsverarbeitung

zwischen

-nachstehend Auftraggeber genannt-

und

Motaev Marx Motaev (MMM) GbR
Vahrenwalder Str. 253
30179 Hannover
Deutschland

-nachstehend Auftragnehmer genannt-

-nachstehend gemeinsam „Parteien" genannt-

Präambel

Im Rahmen dieser Vereinbarung wird mit anwendbaren Datenschutzrecht die Datenschutzgrundverordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten (im Folgenden „DSGVO") und soweit anwendbar, das Bundesdatenschutzgesetz in der geltenden Fassung (im Folgenden „BDSG ") gemeint.

Zur Wahrung und Konkretisierung der Rechte und Pflichten soll diese Vereinbarung nach dem Willen der Parteien den Anforderungen einer Auftragsdatenverarbeitung gemäß Art. 28 Abs. 3 DSGVO genügen. Im Zweifel ist sie so auszulegen, wie sie den Bedingungen anwendbaren Datenschutzrechts zum maßgeblichen Zeitpunkt entspricht.

§ 1 Gegenstand und Dauer Auftrags

(1) Der Gegenstand des Auftrags ist das Hosting, die Breitstellung und der Support eines online-basierten Tools zur Entwicklung von Online-Umfragen und der vorübergehenden Erhebung, Verarbeitung und Nutzung (im Folgenden „Verarbeitung") von personenbezogenen Daten im Sinne des Art. 4 Nr. 1, 2 DSGVO zur Auswertung der Rückmeldungen.

(2) Der Auftrag zur Verarbeitung ist unbefristet erteilt und kann von den Parteien mit einer Frist von einem Monat zum Monatsende gekündigt werden.

§ 2 Zweck der Verarbeitung

Zu Marketingzwecken werden regelmäßige Fragebögen für Umfragen an betroffene Personen über das Online Tool erstellt. Die Rückantworten des Personenkreises werden über einen Link direkt auf dem Web-Interface des Auftragnehmers eingegeben. Der Auftraggeber kann über das Web-Interface die Daten auswerten, sie bearbeiten, herunterladen und ggf. löschen.

§ 3 Art der Daten und Kreis der betroffenen Personen

Die Art der Daten betreffen Vor- und Nachnamen, sowie Kommunikationsdaten der betroffenen Personen. Mit betroffenen Personen sind Endkunden (B2B) und Geschäftskunden (B2C) sowie Geschäftspartner, Interessenten, Lieferanten, Dienstleister, Mitarbeiter und andere Besucher des Auftragsgebers gemeint.

§ 4 Rechte und Pflichten des Auftraggebers

(1) Soweit in dieser Vereinbarung nicht anders geregelt, ist der Auftraggeber als Verantwortlicher im Sinne des Art 4 Nr. 7 DSGVO für die Einhaltung gesetzlicher Bestimmungen des Datenschutzes gem. Art. 24 DSGVO, insbesondere der Rechtmäßigkeit der Datenweitergabe an den Auftragnehmer sowie der Datenverarbeitung nach Art. 6 Abs. 1 DSGVO verantwortlich und bestimmt die Zwecke und Mittel der Verarbeitung (Weisungsbefugnis).

(2) Die Verarbeitung personenbezogener Daten erfolgt auf dokumentierte Weisung des Auftraggebers. Zudem darf der Auftragnehmer, sofern deutsches Recht oder das Recht der Europäischen Union hierzu verpflichtet, personenbezogene Daten verarbeiten. Im Falle des Satz 2 dieses Absatzes hat der Auftragnehmer den Auftraggeber zu informieren und etwaige Auskünfte nach vorheriger schriftlicher Zustimmung durch den Auftraggeber zu erteilen.

(3) Mündliche Weisungen sind unverzüglich in Textform zu bestätigen. Jegliche Weisungen sind zu Dokumentieren.

(4) Ist der Auftragnehmer der Auffassung, eine Weisung verletze geltendes Datenschutzrecht nach Art. 33 Abs. 1 S. 1 DSGVO oder Art. 34 Abs. 1 DSGVO, hat er den Auftraggeber unverzüglich in Kenntnis zu setzen. Bis zur Bestätigung oder Änderung der Weisung ist der Auftragnehmer berechtigt, die Durchführung auszusetzen.

§ 5 Vertraulichkeitsverpflichtung

Der Auftragnehmer verpflichtet sich, bei der Verarbeitung nur Beschäftigte einzusetzen, die mit den für sie relevanten Datenschutzbestimmungen vertraut und auf das Datengeheimnis und auf die Vertraulichkeit verpflichtet worden sind.

§ 6 Datensicherheit

(1) Der Auftragnehmer verpflichtet sich gemäß Art. 28 Abs. 3 S. 2 lit. c DSGVO und Art. 32 DSGVO, angemessene technische und organisatorische Maßnahmen in Übereinstimmung mit dem anwendbaren Datenschutzrecht zu ergreifen, zu gewährleisten und zu dokumentieren.

(2) Bei den zu treffenden Maßnahmen der Datensicherheit und Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, Integrität und Verfügbarkeit von Daten sind insbesondere die Risiken zu berücksichtigen, die mit der Verarbeitung verbunden sind. Unter anderem:

a. Zugangskontrolle
b. Datenträgerkontrolle
c. Speicherkontrolle
d. Benutzerkontrolle
e. Zugriffskontrolle
f. Übertragungskontrolle
g. Eingabekontrolle
h. Transportkontrolle
i. Wiederherstellbarkeit
j. Zuverlässigkeit
k. Datenintegrität
l. Auftragskontrolle
m. Verfügbarkeitskontrolle

n. Trennbarkeit

(3) **Anhang 1** ist Bestandteil dieser Vereinbarung

(4) Der Auftragnehmer sichert dem Auftraggeber zu, die in **Anhang 1** erläuterten technischen und organisatorischen Maßnahmen tatsächlich umgesetzt zu haben. Zudem sichert er zu, dass die vorgenannten technischen und organisatorischen Maßnahmen den Anforderungen des Abs. 1 und 2 dieses Paragraphen und den Anforderungen des anwendbaren Datenschutzrechts entsprechen.

(5) Dem Auftragnehmer ist es gestattet, alternative adäquate Maßnahmen zu ersetzen, sollte technischer Fortschritt und Weiterentwicklung dies gebieten. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden.

§ 7 Unterauftragsverhältnisse

(1) Der Auftraggeber erteilt dem Auftragnehmer die Vorabgenehmigung zur Bereitstellung von Servern mit sicheren und hochverfügbaren Rechenzentren an

1&1 IONOS SE
Elgendorfer Straße 57
56410 Montabaur

unter der Bedingung der Einhaltung der weiteren Anforderungen dieses Paragraphen (**Anhang 2**). Die Beauftragung weiterer Unterauftragsnehmer durch den Auftragnehmer ist grundsätzlich verboten und steht unter dem Genehmigungsvorbehalt des Auftraggebers.

(2) Eine weitere Unterbeauftragung durch den Unterauftragnehmer bedarf der ausdrücklichen im Voraus einzuholenden Genehmigung durch den Hauptauftraggeber unter Einhaltung der Textform.

(3) Der Auftragnehmer hat die vertragliche Vereinbarung mit Unterauftragnehmern derart zu gestalten, dass sie den Datenschutzbestimmungen im Vertragsverhältnis zwischen Auftraggeber und Auftragnehmer entsprechen.

§ 8 Betroffenenrechte

(1) Der Auftragnehmer ist verpflichtet, den Auftraggeber bei der Wahrung Betroffenenrechten gemäß Art. 12 bis 22 DSGVO zu unterstützen.

(2) Soweit die betroffene Person gegenüber der verantwortlichen Stelle ein Recht geltend machen kann, stellt der Auftragnehmer sicher, dass der Auftraggeber die verarbeiteten personenbezogenen Daten in einer lesbaren Form erhalten kann.

(3) Der Auftragnehmer darf personenbezogene Daten gem. § 62 Abs. 5 S. 2 Nr. 1 BDSG sowie Art 28 Abs. 3 S. 2 lit. a DSGVO nur nach dokumentierter Weisung des Auftraggebers herausgeben, berichtigen, löschen oder deren Verarbeitung einschränken. Auskünfte und Ersuche betroffener Personen sind erst nach vorheriger schriftlicher Zustimmung durch den Auftraggeber zu erteilen.

§ 9 Rechte und Pflichten des Auftragnehmers

(1) Der Auftragnehmer ist nicht zur Benennung eines Datenschutzbeauftragten verpflichtet. Als Ansprechpartner für Themen des Datenschutzes wird

Herr Dipl.-Jur. David Motaev
E-Mail: datenschutz@questionstar.de

Telefon: 0511 856 439 94

benannt. Der Ansprechpartner für Themen des Datenschutzes muss auf Anfrage des Auftraggebers in der Lage sein, den Nachweis zu erbringen, dass die Vorgaben anwendbaren Datenschutzrechts eingehalten werden.

(2) Dem Auftragnehmer sind die nach anwendbarem Datenschutzrecht bestehenden Meldepflichten bekannt und ist verpflichtet, sich über gesetzliche Meldepflichten fortlaufend zu informieren.

(3) Der Auftragnehmer hat dem Auftraggeber über alle Fälle datenschutzrechtlicher Verstöße oder bei hinreichend begründetem Verdacht dazu in Kenntnis zu setzen.

(4) Der Auftragnehmer unterstützt den Auftraggeber bei der Aufklärung und Identifizierung von Auswirkungen sowie bei der Dokumentation des Vorfalls und zu ergreifenden Abhilfemaßnahmen. Insgesamt verpflichtet sich der Auftragnehmer, den Auftraggeber bei der Einhaltung der in Art. 32-36 DSGVO genannten Pflichten zu unterstützen.

(5) Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf schriftliche Anforderung innerhalb einer angemessenen Frist alle Auskünfte und Nachweise zur Verfügung zu stellen, die zur Durchführung einer Kontrolle im schriftlichen Verfahren erforderlich sind. Über die Kontrolle und deren Ergebnisse ist vom Auftraggeber ein Protokoll anzufertigen.

§ 10 Haftung

(1) Für den Ersatz von Schäden, die eine betroffene Person wegen einer unzulässigen oder unrichtigen Verarbeitung im Auftrag dieser Vereinbarung erleidet, ist der Auftraggeber verantwortlich.

(2) Soweit der Auftraggeber zum Schadensersatz gegenüber einer betroffenen Person verpflichtet ist, bleibt ihm der Rückgriff auf den Auftragnehmer vorbehalten, wenn der Auftragnehmer gegen Pflichten aus dieser Vereinbarung oder anwendbarem Datenschutzrecht schuldhaft verstoßen hat.

§ 11 Drittländer

Die Verarbeitung und Nutzung der Daten findet ausschließlich im Gebiet der Bundesrepublik Deutschland, einem Mitgliedsstaat der Europäischen Union oder einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die Voraussetzungen anwendbaren Datenschutzrechts erfüllt sind.

§ 12 Beendigung des Auftrags

(1) Der Auftragnehmer hat gem. Art. 28 Abs. 3 lit. g. DSGVO nach Abschluss der Erbringung der Verarbeitungsleistung nach Wahl des Auftraggebers alle personenbezogenen Daten zu löschen oder zurückzugeben.

(2) Dokumentationen, die dem Nachweis der ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren.

§ 13 Berufsgeheimnis

Der Auftragnehmer verpflichtet sich, die strafbewehrten Verschwiegenheitspflichten sowie das Datengeheimnis besonders sorgfältig zu wahren.

§ 14 Schlussbestimmungen

(1) Überlassene Datenträger und Datensätze verbleiben im Eigentum des Auftraggebers

(2) Sollten einzelne oder mehrere Regelungen dieser Vereinbarung unwirksam sein, so bleibt die Wirksamkeit der übrigen Vereinbarung davon unberührt. In einen Fall des Satz 1, werden die Vertragsparteien die unwirksame Regelung unverzüglich durch eine ersetzen, die der Regelung wirtschaftlich und datenschutzrechtlich am ehesten entspricht.

(3) Soweit andere Vereinbarung zum Zeitpunkt des Abschlusses dieses Vertrages anderslautende oder diesem Vertrag widersprechende Angaben erhalten, so gehen die Inhalte dieses Vertrages vor.

(4) Die folgenden Anhänge sind Bestandteil dieser Vereinbarung

- Anlage 1 „Technische und organisatorische Maßnahmen"
- Anlage 2 „Durch 1&1 Internet SE gesicherte Maßnahmen und Zertifikate"

_____ _____

Datum, Unterschrift Auftraggeber Datum, Unterschrift, Auftragnehmer

Anhang 1

Technische und organisatorische Maßnahmen

1. Zutrittskontrolle

Hochsicherheitsrechenzentrum (1und1 AG, Karlsruhe), mit eingeschränkter Zutrittsberechtigung nur für technisches Personal von 1und1 AG. Elektronische und physische Zutrittskontrollen in Server- Zentrum

2. Zugangskontrolle

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

3. Zugriffskontrolle

Alle Daten, welche von QUESTIONSTAR verarbeitet werden, werden in einer redundanten, verteilten und replizierten Hochleistungsdatenbank des führenden Datenbankherstellers gespeichert und mehrfach gesichert. Die Daten werden verschlüsselt gespeichert und sind durch zahlreiche technische Systeme geschützt.

Administrator-Bereich und optional auch Ihre Befragungen werden mit der derzeit höchsten verfügbaren Secure Socket Layer Verschlüsselung (256 Bit SSL Verschlüsselung) vor fremden Einblicken auch via Sniffer-Software abgeschirmt. Bei Verwendung von SSL-Verschlüsselung sind 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. Eindeutige (persönliche) Zuweisung von Zugriffsberechtigungen mit persönlichen Passwörtern. Zuordnung von Verantwortlichkeiten. Protokollierung der Systemnutzung. Verpflichtung der Mitarbeiter auf Datengeheimnis nach § 5 BDSG. Die Sicherheit unserer Server-Systeme gegenüber externen ungewollten Zugriffen wird von zentralen Firewalls übernommen. Das Netzwerk selbst verfügt dabei selbst über einen sicheren privaten Adressbereich. Remotezugriffe für unsere Administratoren geschehen werden mit Protokollen mit Datenverschlüsselung (SSH) und weiteren Sicherheitsmaßnahmen geschützt.

4. Weitergabekontrolle

Beim Aufruf von den durch die Fragebogen gesammelten Daten über SSL-verschlüsselte Verbindung, werden die Daten diese wie im Punkt 3 beschrieben geschützt mit mindestens 256 Bit Verschlüsselung zwischen unserer Datenbank und dem Rechner der Kunden übertragen.

5. Eingabekontrolle

Login-Logout-Protokolle mit IP, Browserangaben, etc. Protokollierungsverfahren von Starts und Stopps von Umfragen durch den Kunden in dessen Admin-Bereich.

6. Auftragskontrolle

Regelungen der Zweckbindung der Datennutzung durch den Auftraggeber sowie durch unsere AGB unter www.questionstar.de/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.

7. Verfügbarkeitskontrolle

Wir unterhalten redundante, sichere Systeme mit regelmäßiger Datensicherung auf redundanten Storage-Medien, unterbrechungsfreie Stromversorgung auf Enterprise-Level (USV) durch Notstrom- Diesel-Aggregat und Blei-Gel-Batterien, Internen-Gas-Brandschutz-Anlage. Wir überwachen unsere Systeme permanent mit Alert-Monitor. Alle Server dienste werden regelmäßig mit verschiedenen Notszenarien überprüft und mögliche Systemunterbrüche proaktiv festgestellt und umgehend behoben.

8. Trennungskontrolle

Mandantentrennung und Trennung der Nutzer eines Mandanten über Regelung der Zugriffsrechte im Admin-Bereich (Onlinezugriff) in unterschiedlichen Nutzerkonten bzw. Multi-User-Zugriffen (getrennte Berechtigungen für verschiedene Umfragen).

Anhang 2

Durch 1&1 Internet SE gesicherte Maßnahmen und Zertifikate

TÜV NORD

ZERTIFIKAT

für das Managementsystem nach
ISO/IEC 27001 : 2013
(Einschließlich Cor 1:2014 und Cor 2:2015)

Die Zertifizierungsstelle TÜV NORD CERT GmbH bestätigt hiermit als Ergebnis der Auditierung, Bewertung und Zertifizierungsentscheidung gemäß ISO/IEC 27006:2015/Amd.1:2020, dass die Organisation

IONOS Holding SE
c/o IONOS SE
Elgendorfer Straße 57
56410 Montabaur
Deutschland

IONOS

ein Managementsystem konform zu den Anforderungen der ISO/IEC 27001 : 2013 betreibt und innerhalb der Laufzeit des Zertifikats von 3 Jahren auf Konformität überwacht wird.
Bei dem zertifizierten Managementsystem handelt es sich um das der gesamten zertifizierten Organisation.

Geltungsbereich

Betrieb und Entwicklung von Infrastruktur, Plattformen und Applikationen für Internetprodukte und -dienstleistungen in den Rechenzentren der IONOS sowie der zugehörige Kundenservice

Unter Berücksichtigung der Erklärung zur Anwendbarkeit vom 17.02.2022, Version 4.0

Zertifikat-Registrier-Nr. 44 121 160247-012
Auditbericht-Nr. 3531 7732

Gültig von 2022-04-19
Gültig bis 2025-04-18
Erstzertifizierung 2021

Zertifizierungsstelle
der TÜV NORD CERT GmbH

Essen, 2022-04-19

Dieses Zertifikat ist gültig in Verbindung mit dem Hauptzertifikat.
Die Gültigkeit kann unter https://www.tuev-nord.de/de/unternehmen/zertifizierung/zertifikatsdatenbank verifiziert werden.

TÜV NORD CERT GmbH Am TÜV 1 45307 Essen www.tuev-nord-cert.de

IAF MEMBER OF MULTILATERAL RECOGNITION ARRANGEMENT
DAkkS Deutsche Akkreditierungsstelle D-ZM-12007-01-00