Data Processing Agreement

between

_____
_____
_____
_____
_____

– hereinafter referred to as the "Client" –

and

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

– hereinafter referred to as the "Processor" –

– hereinafter jointly referred to as the "Parties" –

Preamble

Within the framework of this agreement, the applicable data protection law refers to the General Data Protection Regulation of the European Parliament and Council for the protection of natural persons with regard to the processing of personal data (hereinafter "GDPR") and, where applicable, the current version of the German Federal Data Protection Act (hereinafter "BDSG").

This agreement is intended to meet the requirements of Article 28(3) GDPR regarding commissioned data processing. In case of doubt, it shall be interpreted in accordance with the applicable data protection law at the relevant time.

§ 1 Subject and Duration of the Commission

(1) The subject of the commission is the hosting, provision, and support of an online-based tool for creating online surveys and the temporary collection, processing, and use (hereinafter "processing") of personal data as defined by Art. 4(1), (2) GDPR for the evaluation of feedback.

(2) The data processing assignment is granted for an indefinite period and may be terminated by either party with one month's notice to the end of a month.

§ 2 Purpose of Processing

For market research purposes, regular questionnaires are created via the online tool and distributed to data subjects. Responses are entered directly via a link into the Processor's web interface. The Client can analyze, edit, download, and delete the data via the web interface.

§ 3 Nature of Data and Categories of Data Subjects

The data includes first and last names as well as contact details of the data subjects. Data subjects include end customers (B2B), business customers (B2C), business partners, prospects, suppliers, service providers, employees, and other visitors of the Client.

§ 4 Rights and Obligations of the Client

(1) Unless otherwise stated in this agreement, the Client, as the controller under Art. 4(7) GDPR, is responsible for complying with the legal provisions on data protection under Art. 24 GDPR. This includes ensuring the lawfulness of the data transfer and processing in accordance with Art. 6(1) GDPR and determining the purposes and means of the processing (right to issue instructions).

(2) The processing of personal data takes place only on documented instructions from the Client. The Processor may only process personal data if required to do so by Union or Member State law; in such cases, the Client must be informed.

(3) Oral instructions must be promptly confirmed in writing. All instructions are to be documented.

(4) If the Processor considers an instruction to be in breach of data protection law under Art. 33(1) or Art. 34(1) GDPR, they must immediately inform the Client. Processing shall be suspended until the instruction is confirmed or modified.

§ 5 Confidentiality Obligation

The Processor agrees to use only employees who are familiar with applicable data protection regulations and have committed themselves to confidentiality and data secrecy.

§ 6 Data Security

(1) The Processor agrees, in accordance with Art. 28(3)(2)(c) and Art. 32 GDPR, to implement appropriate technical and organizational measures and to document these in compliance with applicable data protection law.

These include, but are not limited to:

a. Access control
b. Media control
c. Storage control
d. User control
e. Access control
f. Transmission control
g. Input control
h. Transport control
i. Recoverability
j. Reliability
k. Data integrity
l. Order control
m. Availability control
n. Separation

(2) **Appendix 1** is part of this agreement.

(3) The Processor guarantees that the technical and organizational measures described in **Appendix 1** have been implemented and comply with the applicable legal requirements.

(4) If technological advancements require it, the Processor may introduce alternative adequate measures, provided that the protection level is not reduced.

§ 7 Subcontractors

(1) The Client grants the Processor prior approval to use servers in secure and high-availability data centers provided by:

1&1 IONOS SE
Elgendorfer Straße 57
56410 Montabaur
Germany

(2) Further subcontracting requires the Client's prior written approval. The subcontractor must comply with the same data protection obligations as set out in this agreement.

§ 8 Rights of Data Subjects

(1) The Processor shall support the Client in fulfilling data subject rights under Art. 12–22 GDPR.

(2) The Processor ensures that the Client can access personal data in a readable format upon request.

(3) The Processor may only release, rectify, delete, or restrict personal data following documented instructions from the Client. Requests from data subjects are to be handled only with prior written approval from the Client.

§ 9 Rights and Duties of the Processor

(1) The Processor is not required to appoint a Data Protection Officer. The contact person for data protection matters is

Mr. Dipl.-Jur. David Motaev
Email: datenschutz@questionstar.de
Phone: +49 511 856 439 94

This contact must be able to provide proof of GDPR compliance upon request.

(2) The Processor is aware of and obliged to comply with all applicable legal reporting duties under data protection law.

(3) The Processor shall inform the Client of any personal data breach or well-founded suspicion thereof.

(4) The Processor shall support the Client in clarifying and assessing the impact of such incidents, in documenting the incident, and in implementing appropriate remedial measures. Furthermore, the Processor undertakes to assist the Client in complying with the obligations set out in Articles 32 to 36 of the GDPR.

(5) The Processor undertakes to provide the Client, upon written request and within a reasonable period, with all information and evidence required for conducting an audit by means of written procedure. The Client shall draw up a protocol of the audit and its results.

§ 10 Liability

(1) The Client is liable for damages suffered by data subjects due to unlawful or incorrect data processing.

(2) If the Client is held liable to a data subject, they may seek recourse against the Processor if the Processor has culpably breached its obligations.

§ 11 Third Countries

Data processing shall take place only within Germany, the EU, or EEA. Transfers to third countries require prior written approval from the Client and must meet all requirements of applicable data protection law.

§ 12 Termination of the Commission

(1) In accordance with Art. 28(3)(g) GDPR, the Processor must delete or return all personal data at the end of the processing services, at the Client's choice.

(2) Documentation proving lawful processing must be retained beyond the termination period according to legal retention periods.

§ 13 Professional Secrecy

The Processor is obligated to uphold statutory confidentiality and data secrecy with the utmost care..

§ 14 Final Provisions

(1) All data carriers and datasets remain the property of the Client.

(2) If individual provisions of this agreement are invalid, the rest remains unaffected. The parties will replace the invalid provision with one that best reflects its intent.

(3) This agreement supersedes any conflicting or previous arrangements.

(4) The following appendices are part of this agreement:

- Appendix 1 "Technical and Organizational Measures"
- Appendix 2 "Measures and Certificates by 1&1 IONOS SE"

_____ _____

Date, Signature Client Date, Signature Processor

Appendix 1
Technical and Organizational Measures

1. Access Control

High-security data center (1&1 IONOS SE), with restricted physical access granted only to technical personnel of 1&1 IONOS SE. Electronic and physical access controls are in place at the server center.

2. System Access Control

Password protection for all essential technical systems, logging of the use of all key systems and processes, and log monitoring by management.

3. Data Access Control

All data processed by QUESTIONSTAR is stored in a redundant, distributed, and replicated high-performance database provided by a leading database vendor and is securely backed up multiple times.
The data is stored in encrypted form and protected by numerous technical systems.

The administrator area—and optionally also your surveys—are protected from external access (e.g., sniffer software) by the highest currently available Secure Socket Layer encryption (256-bit SSL).
Using SSL encryption ensures that all data transfers between the participant's local computer and our database are encrypted and fragmented with the same security used by banks and insurance companies, making the content unreadable.

Additional measures include:

- Limiting access only to data required for specific employee tasks (segmentation)
- Granular user permissions
- Personal access credentials (passwords)
- Responsibility assignments
- Logging of system usage
- Employee confidentiality obligations according to §5 BDSG
- Protection against external access via centralized firewalls
- Use of a secure private network address range
- Remote administrator access secured via encrypted protocols (SSH) and additional security measures.

4. Data Transfer Control

When survey data is accessed via an SSL-encrypted connection, the transfer is protected as described in Section 3 with at least 256-bit encryption between our database and the client's computer.

5. Input Control

Login/logout logs with IP addresses, browser data, etc. Logging of survey starts and stops in the client's admin area.

6. Job Control

Binding data use to agreed purposes via contract and our Terms & Conditions at https://questionstar.com/terms-of-service. Data is used solely for agreed purposes (e.g., data collection, delivery, execution, statistical evaluation, export for the client). Upon request, data can be permanently deleted by us, including a deletion log.

7. Availability Control

We operate redundant, secure systems with regular data backups to redundant storage media, enterprise-level uninterruptible power supply (UPS) via diesel generator and lead-gel batteries, internal gas fire suppression systems, and constant system monitoring with alert monitors. All server services are tested regularly with various emergency scenarios to proactively detect and promptly resolve any service interruptions

8. Separation Control

Tenant separation and user-level data access controls are enforced in the admin interface (online access) through separate user accounts and multi-user access with differentiated permissions for various surveys.

Appendix 2

Measures and Certificates Secured by 1&1 IONOS SE

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