DATA PROCESSING AGREEMENT

Customer
Company name: .....

Contact person: .....

Email: .....

Questback

This Data Processing Agreement ("DPA") forms part of Questback's provision to Customer of access to Software and related services (jointly referred to as the "Services"), as further specified in the applicable agreement between Customer and Questback, and all documents and exhibits incorporated therein (jointly referred to as the "Agreement"). Questback will carry out processing of Personal Data on behalf of the Customer in accordance with the terms of this DPA, its exhibits, the Agreement and applicable Data Protection Legislation.

The parties agree that Questback is the Processor of Personal Data under this DPA, and Customer is the Controller as defined in GDPR Article 4. In case Customer is entitled pursuant to the Agreement to use the Services for the benefit of any third party, Customer may be the Processor, while Questback may be the Sub-processor.

1. Definitions

In this DPA, all capitalized terms shall have the meanings set out in, and will be interpreted in accordance with this DPA, the GDPR and applicable Data Protection Legislation.

Agreement means the separate agreement(s) between Questback and the Customer where the content and scope of the Services provided by Questback to Customer is agreed.

Data Protection Legislation means the laws, statutes, enactments, regulations, directives, standards and other similar instruments from time to time that apply in relation to the Processing of Personal Data.

GDPR means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons regarding the processing of Personal Data and on the free movement of such data, and repealing Directive 95/46/EC.

Respondent means an individual who provides data by entering data into surveys made available to them by Customer.

Software means the standard online software to which Customer is granted access in the Agreement.

Sub-processor means any third party subcontractor, including Questback Affiliates, engaged by Questback which processes Personal Data on Questback's behalf.

Questback Affiliates mean members of the Questback Group that may assist in the performance of the Agreement.

Questback Group means, for the purpose of this DPA, Questback Holding AS, Questback AS, and any wholly or fully owned subsidiaries of Questback AS.

2. Customer Obligations

2.1 Customer remains at any times responsible for compliance with its obligations as Controller or Processor under this DPA and applicable Data Protection Legislation.

2.2 In particular, Customer will:

2.2.1 Ensure that the information in Appendix A ("Description of Data and Processing") is correct, complete, and updated if necessary (e.g. new survey projects).

2.2.2. Provide all information and notifications to Data Subjects that are required under Data Protection Legislation in due time.

2.2.3 Ensure that it has and always maintains a lawful basis in accordance with applicable Data Protection Legislation for processing of all Personal Data it performs using the Services (including obtaining valid informed consents from Data Subjects).

2.2.4 Inform Questback without undue delay in the event i) the legal basis for Customer's data processing in accordance with applicable Data Protection Legislation ceases to exist (e.g. withdrawal of consent by Data Subject), and ii) Customer obtains information that create suspicion of unauthorized access to or handling of Personal Data. Customer shall provide all relevant information. Section 9 of this DPA applies accordingly.

3. Questback Obligations

Questback shall at all times fulfil its responsibilities as Processor under applicable Data Protection Legislation, in particular, Questback will:

3.1 Process the Personal Data only on documented written instructions from the Customer. Unless otherwise specified, Questback will perform the initial instructions set forth in the Agreement. Questback will immediately inform Customer if, in its opinion, any instruction infringes applicable Data Protection Legislation, and suspend further processing until Customer confirms the legality of processing the data in writing.

3.2 ensure that persons authorized to process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

3.3. take into account the nature of the processing, assist the Customer by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of the Customer's obligation to respond to requests for exercising the Data Subject's rights laid down in GDPR Chapter III.

3.4 assist the Customer in ensuring compliance with the obligations pursuant to GDPR Articles 32 to 36 taking into account the nature of processing and the information available to the Processor.

3.5 make available to the Customer all information necessary to demonstrate compliance with the obligations laid down in GDPR Article 28 and allow for audits by the Customer.

3.6 assist the Customer in ensuring compliance with applicable law, including assisting the Customer with complying with duty of notification to Supervisory Authorities and Data Subjects in case of a Personal Data Breach.

Assistance as set out above, shall be carried out to the extent necessary, taking into account the Customer's need, the nature of the processing and the information available to the Processor.

4. Technical and Organizational Measures, IT Security

4.1 When processing Personal Data on behalf of Customer in connection with fulfilment of the Agreement, Questback shall ensure that it implements and maintains appropriate technical and organizational security measures for the processing of such data taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons.

4.2 Appropriate technical and organizational measures to ensure a level of security appropriate to the risk may include the pseudonymization and encryption of Personal Data, the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services, the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident, and a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

4.3 In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data transmitted, stored or otherwise processed.

4.4 Questback shall take steps to ensure that any natural person acting under Questback's authority who has access to Personal Data does not process them except on instructions from the Customer, unless he or she is required to do so by applicable Data Protection Legislation.

4.5 Customer acknowledges and agrees to Questback's technical and organizational measures as documented, which are continuously updated and posted on Questback's website https://insights.questback.com/data-privacy-and-security. Questback is entitled to change, adjust, modify, update or replace any of its technical and organizational measure, provided however that the level of data protection and security may not be compromised.

5. Administration of Personal Data

5.1 Questback will at all times grant Customer, as agreed in the Agreement, electronic access to the online Software platform that holds Customer's Personal Data, allowing Customer to delete, release, correct, export, save or block access to specific Personal Data, as Customer requires.

5.2 Customer may, to the extent permitted by applicable law, provide detailed written instructions to Questback to delete, release, correct, export, save or block access to Respondent Personal Data. If Customer requires Questback to perform such deletion, release, correction, export, saving or blocking of access to data that Customer could itself have performed, Customer agrees to pay Questback's then-current fees associated with such performance.

6. Data Transfer to countries outside EEA

6.1 Questback will not transfer Personal Data outside the EEA, to any country or recipient: (i) not recognized by the European Commission as providing an adequate level of protection for Personal Data, or (ii) not covered by a suitable safeguard recognized by the relevant authorities or courts as providing an adequate level of protection for Personal Data, including but not limited to Binding Corporate Rules, Binding Corporate Rules for Processors and EU Standard Model Clauses. To ensure an adequate protection of Customer 's Personal Data, Customer acknowledges that Questback may enter into EU Standard Model Clauses with its Sub-processor on behalf of Customer and facilitate all instructions.

6.2 If Customer, or a party on Customer's behalf, will access Personal Data stored in Questback's storage area in the EEA, or transfer Personal Data stored in Questback's storage area in the EEA from, the EEA storage area, it is Customers responsibility to ensure that either the transfer of data takes place based on a adequacy decision by the European Commission as defined in GDPR Article 45, or appropriate safeguards defined in GDPR Article 46 are in place for such access or transfer.

7. Sub-processors

7.1 Customer agrees that Questback may use Sub-processors to provide its Services and fulfil its contractual obligations under the Agreement and this DPA.

7.2 Questback's website provides a full list of its Sub-processor that are currently engaged by Questback to carry out processing activities on behalf of Customer. The list is available at https://insights.questback.com/data-privacy-and-security and will be continuously updated. Customer consents to Questback's use of Sub-processors as described in this Section.

7.3 Questback will i) restrict the Sub-processor's access to Personal Data only to what is necessary to maintain the Services or to provide the Services to Customer; ii) enter into a written agreement with the Sub-processor and will impose on the Sub-processor

similar contractual obligations that Questback has under this DPA, in particular providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that the processing of Personal Data meets the requirements of the Data Protection Legislation; and (iii) Questback will remain responsible for its compliance with the obligations of this DPA and for any acts or omissions of the Sub-processors that cause Questback to breach any of Questback's obligations under this DPA.

7.4 If Questback plans to engage any new Sub-processor, Questback will notify Customer before engaging the new Sub-processor. The notification may be sent to the email address given at the top of this DPA.

7.5 Customer is entitled to object to the intended engagement within 30 days upon the receipt of a written notification. If Customer does not object to the intended engagement, the change of Sub-processor is deemed as accepted.
In case Customer objects to the engagement, Questback will work with Customer in good faith to find a mutually acceptable resolution to address such objection, e.g. by providing additional documentation to support Questback's compliance with Data Protection Legislation, or by delivering the Services without engaging the new Sub-processor.
If the Parties do not reach a mutually acceptable solution within a reasonable time, (1) Questback is entitled to terminate this DPA and the Agreement with 30 days' notice if the provision of the Services with the original Sub-processor is impossible or commercially unreasonable; (2) Customer is entitled to terminate this DPA and the Agreement with 30 days' notice if there are objective and proven grounds related to the ability of such Sub-processor to adequately process Personal Data in accordance with this DPA or applicable Data Protection Legislation.

8. Audit

8.1 Customer may audit Questback's compliance with the terms of the Agreement and this DPA up to once per calendar year, or to the extent required by applicable law. If a third party is to conduct the audit, the third party must be mutually agreed to by Customer and Questback, except if such third party is a Supervisory Authority. Questback will not unreasonably withhold its consent to a third party auditor requested by Customer. Any person conducting the audit on behalf of Customer, either its employees or a third party, must execute a written confidentiality agreement acceptable to Questback before conducting the audit, or otherwise be bound by a statutory or legal confidentiality obligation towards Questback.

8.2 To request an audit, Customer must submit a written notification at least two weeks in advance of the proposed audit date to Questback describing the proposed scope, duration, and start date of the audit.

8.3 The audit must be conducted during regular business hours at the applicable Questback facility, subject to Questback policies, and may not unreasonably interfere with Questback business activities. Questback will make reasonable efforts to provide requested information required for such an audit to Customer or external auditor authorized according to this DPA.

8.4 Customer will provide Questback with any audit reports generated in connection with any audit under this section without extra charge, unless prohibited by law. Customer may use the audit reports only for the purposes of meeting its regulatory audit requirements and/or confirming compliance with the requirements of the Agreement and this DPA. The audit reports are confidential information of the parties under the terms of the Agreement.

8.5 If the requested audit scope is addressed in a recognized and valid certification issued by a qualified third party auditor within the last twelve (12) months and Questback provides such certificate to Customer confirming there are no material changes in the controls audited, Customer agrees to accept the findings as sufficient demonstration of Questback complying with the audit report and this DPA in lieu of requesting an audit of the same controls covered by the report. The provision of any certificate or audit report may subject to a non-disclosure agreement between Customer and Questback.

8.6 Questback may demonstrate its Sub-processors' compliance with their obligations according to Data Protection Legislation by providing adequate certificates (such as ISO or SOC) or audit reports from independent third party auditors that are not older than twelve (12) months. The provision of any certificate or audit report is subject to a non-disclosure agreement between Customer and Sub-processor. Customer agrees to accept the findings as sufficient demonstration of Sub-processor complying with applicable Data Protection Legislation.

8.7 Each party shall bear its own costs of conducting any audit. A mutual reimbursement of costs is excluded.

9. Incident Management and Breach Notification

9.1 Questback evaluates and responds to incidents that create suspicion of unauthorized access to or handling of Personal Data. Questback will work with Customer, within internal Questback lines of business, with the appropriate technical teams and, where necessary, with outside law enforcement to respond to the incident. The goal of the incident response will be to restore the confidentiality, integrity, and availability of the Software environment, and to establish root causes and remediation steps.

9.2 Questback shall without delay, and no later than within 60 hours, upon becoming aware of an accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data processed by Questback, notify the Customer. Where the information is available for Questback, the notification shall at least:

- describe the nature of the Personal Data Breach including where possible, the categories and approximate number of Data Subjects concerned, and the categories and approximate number of Personal Data records concerned;
- communicate the name and contact details of the data protection officer or other contact point at the Processor where more information can be obtained;
- describe the likely consequences of the Personal Data Breach;
- describe the measures taken or proposed to be taken by the Customer to address the Personal Data Breach, including, where appropriate, measures to mitigate its possible adverse effects.

9.3 To the extent required under the GDPR, and upon Customer's request, Questback will assist Customer in its obligation to notify the Supervisory Authority of a Personal Data Breach.

10. Requests from Data Subject

10.1 Considering the nature of the Processing, Questback shall implement appropriate technical and organisational measures to support the Customer's obligation to respond to requests regarding exercising the rights of the Data Subject. Questback shall, to the extent legally permitted, promptly notify Customer if it receives a request from a Data Subject for access to, correction, amendment or deletion of that person's Personal Data. Questback shall not respond to any such Data Subject request without Customer's prior written consent, except to confirm that the request relates to Customer. Questback will forward any request from Data Subjects to Customer.

10.2 To the extent Customer, in its use or receipt of the Services, does not have the possibility to correct, amend, block or delete Personal Data, as required by Data Protection Legislation, Questback shall comply with any reasonable request by Customer to facilitate such actions to the extent Questback is legally permitted to do so.

10.3 Customer hereby instructs Questback to allow, to the extent technically possible, for Customer's access to, and option to edit, the Personal Data from individual Respondents.

10.4 The responsibility for ensuring that Processing is compliant with applicable Data Protection Legislation when Customer accesses and edits Personal Data from individual Respondents remains solely with Customer.

10.5 Questback shall provide Customer with reasonable cooperation and assistance in relation to handling any Data Subject's request to exercise its statutory rights, to the extent legally permitted and to the extent that Customer has no means of satisfying those rights by using the Software or Services itself.

10.6 Questback may not disclose or provide access to the Data Subject's Personal Data to third parties. Should a request for such disclosure or access be directed to Questback, Questback shall forward this request to Customer.

11. Personnel

Questback shall ensure that its personnel engaged in the processing of Personal Data are informed of the confidential nature of the Personal Data, have a legitimate need to access Personal Data to meet Questback's obligations under the Agreement and this DPA, have received appropriate training on their responsibilities, and are subject to obligations of confidentiality and such obligations survive the termination of that persons' engagement with Questback.

12. Data Protection Officer

Where such appointment is required by Data Protection Legislation, Questback Group have appointed data protection officer(s) that may be contacted at dataprotectionofficer@questback.com. For further contact details, please visit Questback's website at https://insights.questback.com/data-privacy-and-security.

13. Deletion of Personal Data

Questback's Services provide Customer with controls that Customer may use to retrieve, rectify or delete Personal Data as described in the documentation. Following termination of the Agreement, Questback will delete all Personal Data within its due course of business and in accordance with Questback's then-current deletion routines, but no later than 60 days, except as may be required by law. Customer is responsible for exporting its Personal Data prior to the termination of its Agreement.

14. Questback's legitimate business interest

Questback may process Personal Data for its legitimate business interest which consists of: i) billing and account management, compensation (e.g. employee commission, partner incentives) and internal reporting and modelling (e.g. forecasting, revenue, capacity planning, product strategy); ii) prevention and detection of fraud, cybercrime, cyberattacks and other security related incidents that affect Questback's products and services and Customer's data; iii) research, development and product management, i.e. statistical analysis of utilization and performance for testing, quality assurance, benchmarking, tutored services, bot programming, AI development, machine learning etc. to enhance the overall user experience of Questback's products and service. To the extent possible, Questback will only use de-identified, aggregated data to facilitate its legitimate business purposes described herein.

15. Choice of law and legal venue

15.1 This DPA and any dispute or claim arising out of or in connection with it or its subject matter shall be governed by and construed in accordance with the laws defined in the Agreement. The courts defined in the Agreement shall have exclusive jurisdiction over any dispute or claim arising out of or in connection with this DPA or its subject matter.

15.2 If the choice of law under the Agreement is the laws of a country outside the EEA, the laws of Norway will govern this DPA, and any disputes that arise out of or are related to this DPA. The parties then submit to the exclusive jurisdiction of any court sitting Norway for the purpose of any action that arises out of or relates to this DPA brought by any party hereto.

16. Signature

The individuals signing below represent they have authority to bind the named parties to this Data Processing Agreement.

	Name of Customer	Questback
Name in print:		Marc Oetzel, LL.M.
Title:		Group General Counsel
Date:		25.05.2020
Signature:		

Appendices: Appendix A – Description of Data and Processing

APPENDIX A - DESCRIPTION OF DATA AND PROCESSING

In order to comply with the requirements of Data Protection Legislation, the parties must document certain details related to the Personal Data that will be processed.

Subject-matter of the processing

The subject-matter of the processing is Questback's provision of access to its Software to Customer, in order to make Customer able to collect, process, store and analyze feedback in Questback's Software in accordance with the Agreement. If applicable in the Agreement, the subject-matter includes provision of Support, Advisory Services and Professional Services related to Customer's access to and use of the Software.

Duration of the processing

The duration of the processing is defined by the Customer when using the Software on a case-by-case basis. Personal Data will be stored for as long as required i) to fulfill all obligations deriving from the execution of the Agreement, this DPA or, if applicable, any additional agreements between Customer and Questback, or ii) by applicable Data Protection Legislation. Personal Data will be deleted by Questback in accordance with its then-current deletion routine, but no later than 60 days upon the expiration of the Agreement, except as may be required by Data Protection Legislation.

Nature of the processing

The Personal Data stored by Customer in the platform provided by Questback under the Agreement will be processed by Questback for project management, consultancy services, survey creation, respondent management, data collection, assessment, evaluation, extraction, reporting and processing of experience data, support inquiries, and maintenance.

Purpose for the processing

Questback shall process Personal Data solely for the purpose of fulfilling of the Agreement with Customer, and shall not otherwise process and use Personal Data for purposes other than those set forth in this DPA, the Agreement, or as instructed in writing by Customer.

Customer is processing Personal Data in the Software for any of its employee or customer experience project, market research, academic research or for any other legitimate purpose determined by Customer individually on a case-by-case basis, or in the Agreement.

The categories of Data Subjects

As the controller, Customer will specify and update the categories of Data Subjects, as Customer sees fit and inform Questback in writing. If Customer has not specified any categories of Data Subjects, the following Categories will be processed:

Customer's employees, contractors and/or other individuals who are authorized by Customer to access and use Software, provided to Customer under the Agreement, on Customer's behalf ("User").

Customer's employees, contractors, clients, customers, panelists and/or other individuals who are invited by Customer and Customer Users to respond to surveys and provide experience data ("Respondents").

The types of Personal Data

As the controller, Customer will specify and update the types of Personal Data, as Customer sees fit and inform Questback in writing. If Customer has not specified any types of Personal Data, the following types will be processed:

Personal Data from Users may include: Name, e-mail address, telephone number, role, area of interest, address, IP address.

Personal Data from Respondents: Any Personal Data relating to Respondents as requested by Customer, such as name, e-mail address, address, telephone number, role, age, date of birth, sex, marital status, number of children, area of interest, employment details, business address, employer, position, IP address, as well as any other Personal Data provided by Respondent e.g. through open text fields.

As the Controller, Customer may choose to collect and process Special Categories of Data, as described in GDPR Article 9, 10. Customer will list such additional or specified categories herein or inform Questback separately in writing.