Questback Group Code of Privacy

This document forms part of Governance in Questback, and is approved by all chairmen in the companies in Questback group, and by Questback's Group Management Team

Version:	2.01
Approved on:	April 26th 2018
Approved by:	Sara Habberstad

Questback HQ
Bogstadveien 54
0366 Oslo
NORWAY

Table of Contents

1. Introduction 3
2. Questback's team responsible for privacy related issues 3
2.1 Board of Directors for Questback Holding AS 3
2.2 Group Management team 3
2.3 Compliance Officer 3
3. Legal basis for processing 3
4. Purposes for processing personal data in Questback 4
5. Information to data subjects 4
6. Executive Documentation of data and measures 4
6.1 Overview 4
6.2 Transfer of personal data to Third Parties/ Sub-Processing 5
6.3 Request for Information from Data Subjects 5
6.4 Correction and deletion 6
7. Routines for new processing of personal data 7
7.1 Responsible parties 7
7.2 System or process assessment 7
7.3 Conclusion 7
7.4 Training 7
8. Processors and sub-processors 7
8.1 Processors and sub-processors within Questback group 7
8.2 External processors and sub-processors 8
9. Records of processing activities 8
10. Risk assessment and Data protection impact assessment 8
10.1 Criteria for risk assessment 8
10.2 Mitigating measures - overview 8
10.3 IT Security and Physical Security 9
10.4 Data Protection Impact Assessment (DPIA) 9
11. Procedures for audit and control 9
11.1 Improvement action and follow up 10

Questback HQ
Bogstadveien 54
0366 Oslo
NORWAY

1. INTRODUCTION

This document forms part of Governance in Questback, and is approved by chairmen in the companies in Questback group, and by Questback's Group Management Team.

In its role as a controller and as processor for personal data, as defined in the REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 (GDPR) it is Questback's obligation to ensure and facilitate that privacy regulations are observed, and that data subjects' rights following the regulations is implemented in all areas of Questback's business.

In its work to ensure the best possible privacy for data subjects, the Questback group is in the process of implementing Binding Corporate Rules (BCR), and Processor Binding Corporate Rules (pBCR) as defined in the GDPR.

The BCR and pBCR documents form an integral part of this document.

The purpose of this document is to provide an overview of the management of Personal Data Protection in Questback.

2. QUESTBACK'S TEAM RESPONSIBLE FOR PRIVACY RELATED ISSUES

2.1 Board of Directors for Questback Holding AS

The Board of Directors is accountable for ensuring that Questback's risks and obligations, hereunder protection of personal data, are adequately and effectively managed and has the responsibility for establishing a strong control environment and systems that fulfils the expectations in the countries where Questback does business, and is consistent with safe and sound business practices.

2.2 Group Management team

As the principal executive body of Questback, Questback's Group Management Team is responsible for maintaining a sound system of internal control that supports the achievement of policies, values and objectives while safeguarding customers, employees, shareholders and other stakeholders. There is an open and receptive approach to mitigating privacy risk.

GMT defines boundaries, principles and directives under which the operative execution of privacy risk management is done, and serves as the escalation and resolution body for controversial operative issues and for highest impact risk areas

2.3 Compliance Officer

The Compliance Officer shall establish a Privacy team consisting of the Global Data Protection Officer, the Group Privacy Officer, Group Information Security Officer and the Process owner(s) for procedures Processing Personal Data. The Privacy team shall meet yearly and discuss the development, implementation and updating of individual data protection policies and procedures, hereunder the need for updating the pBCR and BCR and related sub-policies.

The Global Data Protection Officer has the responsibility for managing privacy in Questback, and reports to Compliance Officer.

3. LEGAL BASIS FOR PROCESSING

The GDPR requires a legal basis to be in place in order for any personal data to be processed.

No processing of personal data will take place in Questback unless legal basis as defined in in GDPR Article 6 is in place.

When the legal basis for processing is no longer in place, all personal data will be anonymized or deleted.

The relevant legal basis for processing personal data is defined in each sub-policy:

- Employee Privacy Policy
- Customer Privacy Policy
- Supplier Privacy Policy
- Visitor Privacy Policy
- Respondent Privacy Policy

Questback HQ
Bogstadveien 54
0366 Oslo
NORWAY

4. PURPOSES FOR PROCESSING PERSONAL DATA IN QUESTBACK

The GDPR dictates that Personal Data can only be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

Such Purposes for processing Personal data is defined in each sub-policy

- Employee Privacy Policy
- Customer Privacy Policy
- Supplier Privacy Policy
- Visitor Privacy Policy
- Respondent Privacy Policy

5. INFORMATION TO DATA SUBJECTS

Information to data subjects will, as a minimum, include the following,:

- The name and address of the Questback entity that is the Controller
- The name and address of the person responsible for data processing within Questback, or Questback's Data Protection Officer
- The purposes of the processing
- the period for which the data will be processed
- the existence of rights to request access, rectification and erasure or to object to the processing
- the right to lodge a complaint with the supervisory authority, and contact details; recipients or categories of recipients of the personal data; and
- any further information necessary to guarantee fair processing.

ref. also BCR document section 2.8 and 3.6 for specific information to types of Data subjects.

All suppliers shall adhere to these rules or similar rules approved by Questback to meet Questback's requirements set herein.

6. EXECUTIVE DOCUMENTATION OF DATA AND MEASURES

This section describes personal data processed in Questback, and Questback's Technical and organizational measures in place for the processing of personal data.

6.1 Overview

In the course of its business, Questback entities process personal data from other Questback entities, Questback customers, Questback employees, applicants to positions, service providers, suppliers, subcontractors, visitors and prospects. For such data, Questback is the Controller. The processing of such data is described in the BCR document, and in the following policies:

- Employee Privacy Policy
- Customer Privacy Policy
- Supplier Privacy Policy
- Visitor Privacy Policy

In addition, Questback entities process personal data in connection with its software products in order for its customers to be able to collect and analyze data. Such data is controlled by Questback's customers, and may be personal data from Questback's customers' end clients, and other respondents to the clients' surveys, as the case may be. For such data, Questback is the Processor. The processing of such data is described in the PBCR document, and in the

- Respondent Privacy Policy

Questback HQ
Bogstadveien 54
0366 Oslo
NORWAY

6.2 Transfer of personal data to Third Parties/ Sub-Processing

6.2.1 Transfer of Respondent data

Any Questback Group Company may be a Sub-Processor of Personal Data, and depending on the location of the Questback Group Company, processing of Personal Data by such Pub-Processors may involve transfers of Personal Data.

Transferring Personal Data to other Group Companies may be done only if an EU Model Clause Agreement is in place with the Customer, or when Questback Binding Corporate Rules for Processors is finally approved. Questback will then process in compliance with Binding Corporate Rules for Processors.

A company in the Questback Group may retain Third Party Sub-Processors, and depending on the location of the Third Party Sub-Processor, processing of Personal Data by such Sub-Processors may involve transfers of Personal Data.

The current list of Third Party Sub-Processors engaged in processing Personal Data is defined in Data Processing Agreement with each customer.

Questback shall provide Controllers with prior notification before a new Sub-Processor begins processing Personal Data.

6.2.2 Transfer of Employee, Customer, Supplier and Visitor Personal Data

Questback shall transfer Employee Data to a Third Party to the extent necessary to serve the applicable Business Purpose for which the Personal Data are Processed (including Secondary Purposes).

Questback shall transfer Customer Data, Supplier Data or Visitor data to a Third Party to the extent necessary to serve the applicable Business Purpose (including the Secondary Business Purposes) or purposes for which the Data Subject has provided Consent.

Third Party Processors may Process Personal Data only if they have a contract with Questback.

This Article sets forth additional rules for the transfers of Personal Data to a Third Party located in a country that is not considered to provide an “adequate” level of protection for Personal Data (Non-Adequate Country).

Personal Data may be transferred to a Third Party located in a Non-Adequate Country only if EU Model clauses are in place, or when Questback Binding Corporate Rules for Processors is finally approved. Questback will then process in compliance with Binding Corporate Rules for Processors. :

6.3 Request for Information from Data Subjects

When Questback receives a request from an individual who requires insight into his or her data, the following steps are followed:

6.3.1 Step 1 – assess whether the request should be managed by Questback or by customer

- If the Data subject who requires insight is a Respondent to a Questback customer, Questback will inform the Data Subject that the controller (Questback’s customer) is the correct point of contact
- Customer has the means to manage the request in the software provided by Questback
- unless the specific situation indicates that the customer should not manage the request.
- If it is found that it is not customer’s responsibility to perform search, the steps below shall be followed.

6.3.2 Step 2 – collect basic information

The following information must be collected from the individual requesting information:

- Ask it the request relates to a survey. If yes, ask which customer performed the survey
- If the request does not relate to a survey, ask for the reason for the request
- The name of the person requesting information
- The e-mail of the person requesting information
- Consent to use the collected information to bring the request further in Questback or to customer

If the listed information is not provided, Questback cannot act on the request.

Questback HQ
Bogstadveien 54
0366 Oslo
NORWAY

6.3.3 Step 3 – route to the correct personnel

Request shall be reported to the following personnel:

- Country or regional Manager for the applicable country or region
- General Counsel
- IT Security Officer
- Data Protection Officer

6.3.4 Step 4 – ensure identification

In order for Questback to perform a search, ensure that the individual can identify him- or herself as the person he or she wishes information about.

6.3.5 Step 5 – perform the search

The search will be performed in the relevant systems, in accordance with Questback's procedure defined in "Guideline for Personal Data Search" as updated from time to time.

6.3.6 Step 5 – Provide information to the individual

Upon completion of search, any Personal Data found shall be provided to the individual without delay.

6.3.7 Step 6 – Delete or correct data according to policy if required by the Data Subject.

If the individual requires that the data is deleted or corrected, such deletion of correction must be performed without undue delay.

6.3.8 Step 7 – Conclude

Conclude the case, delete all data collected or created as part of the case. Short summary of the case, without name details, to be provided to the Data Protection Officer.

6.4 Correction and deletion

Questback's processes to ensure that data is corrected or deleted according to GDPR follows for each category of Data Subjects from guidelines in the following policies:

- Respondent Privacy Policy
- Employee Privacy Policy
- Customer Privacy Policy
- Supplier Privacy Policy

Questback HQ
Bogstadveien 54
0366 Oslo
NORWAY

7. ROUTINES FOR NEW PROCESSING OF PERSONAL DATA

This section describes Questback's routines when a new system or new means of processing data is planned or added.

7.1 Responsible parties

No process or system that includes processing of personal data will at any point take place unless approved by Questback Group Management Team, by General Counsel, by privacy officer or by Global Data Protection Officer.

7.2 System or process assessment

Presentation to one or more of the roles above must include the following:

- A description of the process
- A description of the purpose for processing data
- A description of types of data that will be processed
- A description of the legal basis for processing
- An initial assessment of the processing in the Questback template for system mapping>
- A risk assessment for the processing, based on the <Questback template for risk assessment>
- If risk is found to be higher than "low", possible mitigating measures shall be presented

7.3 Conclusion

Based on the above, a proposal for final decision may be presented to the relevant level of authority in Questback, who will decide whether the processing may take place.

7.4 Training

To ensure that the process is followed, training for all personnel on a regular basis is required.

8. PROCESSORS AND SUB-PROCESSORS

8.1 Processors and sub-processors within Questback group

Within the group, entities provide services to each other as Shared Services; Tasks in the area of IT, software development, deployment and finance.

The entities in the Questback group process personal data on behalf of each other in the following cases:

- Transfer of data to the relevant country where software is hosted
- Consultants employed in one entity may perform support or professional services for customers located in other entities' countries
- Knowledge sharing within the group, necessary to provide support or professional services to customers, or related to suppliers, may contain personal information
- Employee data may be shared between entities when required for the individual employee's agreement
- During support, personnel in local entities may access data stored in other entities' hosting facilities

Customers are informed in contract or otherwise about Questback entities processing personal data by using other Questback entities as its (sub)processors.

Questback HQ
Bogstadveien 54
0366 Oslo
NORWAY

8.2 External processors and sub-processors

When a third party, or a third party provided system, is employed by Questback to process personal data, such party is a processor, or sub-processor, depending on whether Questback is Controller or Processor for the data in question.

In order for Questback to process personal data by using (sub)processors, it is under obligation to inform the data subjects, or controller, as applicable, and to have a data processing agreement with the relevant (sub)processor.

Questback has suppliers for the group, and suppliers in each subsidiary, that are relevant for one country only. Suppliers are handled in each subsidiary, without a centralized system. Questback will set up a centralized system for suppliers, where it is specified whether the supplier processes personal data, insurance that the supplier has a data processing agreement, follows requirements from Questback etc.

Questback's current list of suppliers processing personal data for the group, and for each subsidiary is listed in separate document "Questback_Group_Privacy_System_Mapping_v1.0_07JUL15", as updated from time to time.

9. RECORDS OF PROCESSING ACTIVITIES

Questback performs mapping of its processing of personal data, as required in GDPR article 30. Such mapping is performed in the format of a survey using Questback's own survey tools, provided to all relevant process owners with intervals defined by Questback and through interviews conducted by the Compliance Officer and/or members of the Privacy Team (3.4). Reports of such mapping is kept in Questback's systems and can be made available to data protection authorities upon request.

Reports of such mapping is available in Questback's systems.

10. RISK ASSESSMENT AND DATA PROTECTION IMPACT ASSESSMENT

10.1 Criteria for risk assessment

Questback has assessed the risk of its processing of personal data, in Questback systems, and in (sub)processor/Third Party systems. The purpose of the Risk assessment is to define the correct Technical and Organizational Measures for the processing, as required in GDPR. The risk assessment covers the following elements in information security: Integrity, Availability and Confidentiality. The Risk Assessment is found in the document "Risk Assessment", as updated from time to time.

For types of processing that fall under the requirements in GDPR section 3, a Data protection impact assessment will be performed in accordance with the GDPR.

As a SAAS provider, Questback will have focus on all areas of Information Security. In case of conflict between the elements, however, Questback will prioritize data confidentiality.

10.2 Mitigating measures - overview

Questback implements both organizational and technical risk mitigating measures, as updated from time to time.

10.2.1 Minimum level of security

Security measures shall be implemented so that individuals and systems outside Questback cannot cause incidents with major consequences for the individual's privacy. Furthermore, it shall not be possible for Questback employees without proper tools, resources and sufficient knowledge of safety measures to trigger such events, nor by negligence or by willful misconduct.

As it is not possible, or permissible under contracts, for Questback to control all personal data collected and processed in Questback's systems by Questback's customers, sensitive data may be processed at all times without Questback's knowledge. Questback will therefore proceed under the assumption that all personal data collected by customers may be sensitive. Consequently, disclosure of information may be of great importance to those concerned. It is therefore necessary to ensure the confidentiality.

Questback handles personal information that may be of a sensitive nature to individuals. Delays or failures may cause inconvenience or harm to them, depending on the information. It is therefore necessary to ensure information availability and integrity. Although the data may be perceived as sensitive, the interests of availability and integrity take precedence over considerations of confidentiality. It must be prevented that Questback employees negligently affect the integrity of the records and retrieval of information. Furthermore, it is vital that third parties may not intentionally affect Questback's operational stability.

Questback HQ
Bogstadveien 54
0366 Oslo
NORWAY

10.2.2 Training and information of personnel

Questback will ensure that its personnel are provided with information and training included privacy and information security issues, as part of their onboarding training, and as part of continuous training of all personnel.

Detailed information is in process, and link to specific documents and training routines will be entered upon finalization.

10.3 IT Security and Physical Security

Questback will ensure a high level of IT governance, and ensure that IT operations are handled by professional third parties with high knowledge and skill within the areas on Privacy and Information Security.

Detailed processes for Information Security and Physical Security in Questback is governed in Questback IT Governance Policy.

10.4 Data Protection Impact Assessment (DPIA)

The process of DPIA is carried out in accordance with Art. 35 GDPR and the guidelines published by the Article 29 Working Party (WP29). A DPIA is required when the processing is "likely to result in a high risk for the rights and freedoms of natural persons" (not only data protection and privacy, but may also involve other fundamental rights such as freedom of speech, freedom of thought, freedom of movement, prohibition of discrimination, right to liberty, conscience and religion). Questback conducts its DPIA in the following order:

1. Mapping of all relevant data processes.
2. Pre-Assessment of all data processing based on criteria of Art. 35
    a. Is there an exemption according to GDPR Art. 35 (5) (whitelist)? If yes, no DPIA is required.
    b. If no, is there an exemption according to GDPR Art. 35 (10) (regulated processing operation)? If yes, no DPIA is required.
    c. If no, a DPIRA shall be required in the case of:
        i. processing on a large scale of special categories of data referred to in Article 9(1)
        ii. processing on a large scale of personal data relating to criminal convictions and offences referred to in Article 10
        iii. a systematic monitoring of a publicly accessible area on a large scale
        iv. processing operation is “likely to result in high risks”?

To measure the probability of a high risk, the WP29 has defined several criteria. In most cases, a data controller can consider that a processing meeting two of the following criteria would require a DPIA to be carried out. In general, the WP29 considers that the more criteria are met by the processing, the more likely it is to present a high risk to the rights and freedoms of data subjects, and therefore to require a DPIA, regardless of the measures which the controller envisages to adopt. However, in some cases, a data controller can consider that a processing meeting only one of these criteria requires a DPIA too. The criteria include, subject to modifications in the future,

- evaluation and scoring
- automated-decision making
- systematic monitoring
- sensitive data on a highly personal level
- data processed on a large scale
- matching or combining datasets
- data concerning vulnerable data subjects
- innovative use
- processing in itself prevents data subjects from exercising a right or using a service or a contract

11. PROCEDURES FOR AUDIT AND CONTROL

Each Questback company’s managing of personal data is part of quarterly management review.

Questback Whistle blowing policy applies to all areas of breach in Questback, including the privacy area.

If breach is discovered as part of management review, or as part of revision, report to Information Security officer and to Compliance Officer shall be done without delay.

Questback HQ
Bogstadveien 54
0366 Oslo
NORWAY

11.1 Improvement action and follow up

Any breach shall be assessed by Privacy Officer or Compliance Officer. Report to Group Management Team and Data Protection Officer shall be done without delay.

In cases where reports to authorities, customers or data subjects are required according to applicable law, such report will be performed within the required timeframes.

In cases where report to customers or data subjects are required according to an agreement with customer, such report will be performed within the required timeframes.