questback

TECHNICAL & ORGANIZATIONAL MEASURES FOR DATA PROTECTION

The objective of this document is to provide an overview of the technical and organizational measures in place in Questback to ensure the protection of personal data processed in Questback Group (hereinafter: Questback).

Document owner: Eric M. Roßner
Document version: 1.55
Confidentiality classification: Public
Release date: November 2, 2020

Questback HQ
Bogstadveien 54
0366 Oslo
NORWAY

Table of Contents

Questback HQ
Bogstadveien 54
0366 Oslo
NORWAY

Questback HQ
Bogstadveien 54
0366 Oslo
NORWAY

1. INTRODUCTION

1.1 Software as a Service

Questback provides Software as a Service to its customers.

Questback is a global leader in enterprise feedback management with customers world-wide using its solutions for data collection and analysing as well as acting on business-critical information.

Questback was founded in 2000. The company's headquarters are in Oslo, Norway. Its American headquarters are in New York. It has subsidiaries in six countries and presence in 19 countries, with more than 300 employees globally.

Questback provides separate software platforms: Enterprise Feedback Suite (EFS), Essentials and QUBIE.

Questback makes its software platforms for feedback management available to its customers as software as a service (SaaS) from external data centers, as described in Questback Binding Corporate Rules for processors, and in this document.

Personal data relating to Questback's customers, and respondent data collected and processed as part of the feedback process, is processed in accordance with Questback Group Code of Privacy, Questback Binding Corporate Rules, and the descriptions in this document.

In this document, the sections named "**Software**" demonstrate how protection of personal data is ensured in Questback's Software.

1.2 Questback data centers

Questback makes its software platforms for feedback management available to its customers as software as a service (SaaS) from data centers in Germany and/or USA, depending on the individual contract between customer and Questback.

In this document, the sections named "**Data Center**" demonstrate how protection of personal data in Questback's software is ensured in accordance with these standards implemented at the **Datagroup**, **Amazon, Microsoft** or **Oracle** data centers.

1.2.1 Datagroup

Processing in software platforms in the Data Center in Frankfurt, Germany – personal data relating to Questback's customers, and respondent data collected and processed as part of the feedback process, is hosted on external servers in the data center controlled by DATAGROUP Bremen GmbH, in locations belonging to DATAGROUP Data Center GmbH, Frankfurt am Main. DATAGROUP has been certified, as follows:

- In accordance with to ISO/IEC 27001:2013 (certificate ID: DSC.567.02.2018, valid until February 27, 2021; this certificate is available upon request)
- By the German Federal Office for Information Security (BSI) in accordance with ISO 27001 and on the basis of the "IT-Grundschutz" Certification Process (certificate number: BSI-IGZ-0312-2018, valid until February 9, 2021; this certificate is available upon request).
- In accordance with to ISO/IEC 20000-1:2011 (certificate ID: 20 410 44148 TMS, valid until September 25, 2021; this certificate is available upon request)

1.2.2 Amazon

Processing in software platforms in the data center in Frankfurt, Germany - personal data of Questback's customers in Europe as well as respondent data collected and processed as part of the feedback process are hosted on external servers in the Amazon controlled data center in Frankfurt.

Processing in software platforms in the data center in North Virginia, USA - if so agreed with customer in contract, personal data relating to Questback's customers and respondent data collected and processed as part of the feedback process, is hosted on external servers in the data center controlled by Amazon.

Amazon holds various certificates and attestations.

- Exact details about existing certificates can be found on the information pages provided by Amazon at https://aws.amazon.com/compliance/programs/.

1.2.3 Microsoft

Processing in Software Platforms at the Data Center in the Netherlands and Ireland - When using QUBIE, as contractually agreed, personal data of Questback customers and respondents collected and processed as part of the feedback process is hosted on external servers in the data center controlled by Microsoft.

Microsoft holds various certificates and attestations.

- Exact details about existing certificates can be found on the information pages provided by Microsoft at https://gallery.technet.microsoft.com/Overview-of-Azure-c1be3942.

1.2.4 Oracle

Processing in software platforms in the data center in Frankfurt, Germany - personal data of Questback's customers in Europe as well as respondent data collected and processed as part of the feedback process are hosted on external servers in the Oracle controlled data center in Frankfurt.

Oracle holds various certificates and attestations.

- Exact details about existing certificates can be found on the information pages provided by Oracle at https://www.oracle.com/cloud/cloud-infrastructure-compliance/.

1.2.5 Operators of data centres

Data Center provider	Address	Country
DATAGROUP Bremen GmbH	Mary-Somerville-Straße 8 D-28359 Bremen	Germany
DATAGROUP Data Center GmbH	Hanauer Landstraße 310 60314 Frankfurt am Main	Germany
Amazon Web Services, Inc.	410 Terry Avenue North Seattle WA 98109	USA
Amazon Web Services EMEA SARL	38 Avenue John F. Kennedy, L-1855	Luxembourg
Microsoft Ireland Operations Limited	One Microsoft Place, South County Business Park, Leopardstown, Dublin 18 D18 P521	Ireland
Oracle Deutschland B.V. & Co. KG	Riesstraße 25, 80992 München	Deutschland

1.3 Questback offices

Processing in Questback's Offices and systems - Personal data relating to Questback's employees, customers, visitors and suppliers is processed in accordance with Questback Binding Corporate Rules.

In this document, the sections named "**Offices**" demonstrate how protection of personal data is ensured in Questback's offices and systems.

Further information about the structure of the data storage process as well as contact information concerning the data protection officers of Questback group are available in Questback Binding Corporate Rules, and on Questback.com.

Name of Questback entity	Office address	Country
Questback AS	Bogstadveien 54, 0366 Oslo	Norway
Questback GmbH	Gustav-Heinemann-Ufer 72a 50968 Köln	Germany
Questback OY	Keilaranta 1, 02150 Espoo	Finland
Questback Sweden AB	Kungsgatan 48 111 35 Stockholm	Sweden

Questback Limited	7th Floor, 110 Cannon Street London EC4N 6EU	United Kingdom
Questback, Inc.	575 Lexington Avenue, 14th floor / WeWorks, New York, NY 10022	New York, USA
Questback, Inc.	1330 Lake Robbins Drive #430 The Woodlands, TX 77380	Texas, USA

1.4 Fulfilment of the General Data Protection Regulation (GDPR)

This document describes how Questback fulfils its obligations for processing Personal data on behalf of its customers in accordance with the requirements in the GDPR for Technical and Organizational Measures. The relevant requirements are found in the GDPR articles 5, 17, 19, 24, 25, 28, 29, 32, 33, 35 and 39.

The technical and organizational measures described in this document are set out by Questback, 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 for the rights and freedoms of natural persons, ref. GDPR article 32.

The data centers themselves provide further information in various formats.

1.4.1 Datagroup

On request, the Datagroup provides access to documentation on data protection and information security processes.

According to Article 32 (1) of the EU Data Protection Regulation (DSGVO), all bodies that process personal data are obliged to take appropriate technical and organisational measures, taking into account the state of the art, the implementation costs and the nature, scope, circumstances and purposes of the processing, as well as the different probability of occurrence and severity of the risk to the rights and freedoms of natural persons, in order to ensure a level of protection of the rights and freedoms of natural persons commensurate with the risk.

Datagroup implements the technical and organisational measures for the protection of personal data in accordance with Article 32 Paragraph 1 DSGVO.

Datagroup regularly checks the technical and organisational measures taken to ensure that they correspond to the state of the art and the organisational possibilities. In this respect Datagroup is permitted to implement alternative adequate measures. In doing so, it is guaranteed that the security level of the measures defined in this document is not undercut.

On request, Datagroup allows the inspection of documentation on data protection and information security processes.

1.4.2 Amazon

Amazon has extensive information available through the AWS website.

https://aws.amazon.com/compliance/gdpr-center/

1.4.3 Microsoft

Microsoft Azure maintains an information security program (including the adoption and enforcement of internal policies and procedures) to help protect customer information against accidental or unlawful loss, access or disclosure, to identify reasonably foreseeable and internal security risks and unauthorized access to the Azure network, and to mitigate security risks, including through risk assessment and periodic testing. Microsoft will designate one or more employees to coordinate the information security program and be responsible for it.

Microsoft provides extensive information through the Microsoft Web site.

https://www.microsoft.com/trustcenter/privacy/privacy-overview

1.4.4 Oracle

Oracle has implemented and will maintain appropriate technical and organizational security measures for the processing of personal data to prevent the accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure of or access to personal data.

Questback HQ
Bogstadveien 54
0366 Oslo
NORWAY

These security measures govern all security areas applicable to the Services, including physical access, system access, data access, transmission and encryption („Encryption in Transit“ & „Encryption at Rest“), input, data protection, data separation and security oversight, enforcement and other security controls and measures.

Oracle provides extensive information through the Oracle Web site.

https://www.oracle.com/applications/gdpr/

2. PHYSICAL ACCESS CONTROL

This section describes Questback’s measures that are in place to prevent unauthorized individuals from physically accessing the data processing systems that are employed to process or use personal data:

2.1 Data center

2.1.1 Center in Frankfurt, Germany

The standards of BSI / ISO 27001 certification apply to the data center building:

An alarm system connected to the police. The data center is located on the second floor and has two separate access control mechanisms. A video surveillance system is used to monitor the computer room. In accordance with ISO27001, the cloud providers Amazon, Oracle and DATAGROUP have a physical access authorization concept that can be viewed on site. A two-level access system was installed to control the physical access to the high-security areas of the data center.

Employee access to the data center

Physical access is provided at the request of the team leader and cross-checking is performed by the management of the respective cloud providers. This physical access is set up on a corresponding transponder for the respective employee. In the second stage of the data centre physical access concept, code locks are added for the data centre administrator group "Knowledge". The physical access authorization lists are checked and updated during internal and external ISO27001 audits whenever changes to the physical access authorizations occur.

Third Party Access to Data Centers

Third party access must be requested by authorized Cloud Provider employees, who must also provide a valid business justification for such access. This request will be granted based on the principle of least privilege, i.e. employees must specify in the request to which level of the data center and for how long they need access. These requests are approved by authorized personnel. Access is revoked after the requested period of time has expired. Persons with a visitor badge must present it on arrival at the site and will be registered and accompanied by authorised personnel.

2.1.2 Center in North Virginia, USA

The standards of ISO 27001 certification apply to the data center building:

Alarms are directly connected to the local Fire and Police Departments. Amazon data centers maintain 24x7x365 monitored CCTV coverage, with CCTV/DVRs supporting Data retention for 90 days in line with PCI requirements. Sensitive equipment such as information processing facilities, including customer servers, is housed in secure sub-areas within each data center’s secure perimeter and is subject to additional controls. Two-factor authentication is required to access all data center facilities. Electromechanical locks are controlled by biometric authentication (hand geometry or fingerprint scanner) and key-card/badge. Termination and role-change control procedures are in place so that any physical or logical access rights are removed in a timely manner when access is no longer necessary or appropriate.

Employee access to data centers

Only authorized AWS personnel have access to physical data centers. All employees who require access to a data center must first submit a request for access and a valid business reason. This request is based on the principle of least privilege, i.e., employees must specify in the request which level of the data center they need access to and for how long. The request is reviewed and approved by authorized personnel. Access is revoked at the end of the requested period. Employees with access to a data center are restricted to certain areas by their authorizations.

Third Party Access to Data Centers

Third party access must be requested by authorized AWS employees who must also provide a valid business reason for such access. This request is granted based on the principle of least privilege, i.e., employees must specify in the request at which level of the data center they require access and for how long. These requests are approved by authorized personnel. Access will be revoked at the end of the requested period. Employees with access to a data center are restricted to certain areas by their authorizations. Persons with a visitor badge must present it on arrival at the site and are registered and accompanied by authorized personnel.

2.1.3 Data center in the Netherlands respectively Ireland

Microsoft designs, builds, and operates data centers to strictly control physical access to the areas where your data is stored. Microsoft understands the importance of protecting your data and is committed to protecting the data centers that contain your data. A complete department at Microsoft designs, builds, and operates the facilities that support Azure. This team is responsible for keeping the physical security up to date.

Microsoft takes a multi-layered approach to physical security to reduce the risk of unauthorized users gaining physical access to data and data center resources. Data centers managed by Microsoft have comprehensive layers of protection: Access permission at the facility perimeter, building perimeter, building perimeter, and data center floor.

Microsoft makes the latest information available online:

https://docs.microsoft.com/azure/security/azure-physical-security#physical-security

2.2 Offices

2.2.1 All offices

All Questback offices will adhere to the requirements in the IT Governance Policy, hereunder definition of security zones. The following sections describe specific elements in place for each office.

2.2.2 Oslo, Norway

- Visitors must report at the reception or to an employee with which they have an appointment, and are accompanied in the building by an employee.
- The entrance doors are equipped with a digital locking system, opened by employee key cards only. The Office Manager has the list of activated keys used by employees.

2.2.3 Stockholm, Sweden

- Visitors must report at the reception or to an employee with which they have an appointment, and are accompanied in the building by an employee.
- The entrance doors are equipped with a digital locking system, opened by a code that will be changed on regular short intervals.

2.2.4 Helsinki, Finland

Questback's office is located 10th floor in Keilaranta 1, Espoo. All employees have access to the office floor and public spaces in the building. The company's own premises are always locked. The keys are controlled by the local Office Manager. The Office Manager has the list of activated keys used by employees. In case of new employees, new access key is applied from Office Manager by their manager. Property of Keilaranta 1 assigns applied keys to the Office Manager. The public premises are open Monday to Friday 8 am – 4 pm. Questback's storage is located in the basement of Keilaranta 1 and the mechanical key is controlled by Office Manager and is held in locked locker when not used.

The property of Keilaranta 1 saves key history daily. Keilaranta 1 delivers monthly reports to Office Manager. The Questback office has three (3) security cameras. Two of them are located in the office and one in server room. Picture is taken every time when someone access to premises. The pictures are located in cloud service and are available four (4) months. Country Manager, IT Manager and Office Manager have access to the web service (http://surveillance.fennoturvapalvelut.com/valvonta/index.php). Customers are not allowed in office premises, exceptions are approved by the members of Management Team. The property of Keilaranta 1 is equipped a number of security cameras as well which are controlled by Securitas Oy.

All Questback employees have an ID card with full name, picture and employee number. Office Manager holds the list of employee numbers. The ID card is equipped with a neck strap. Office Manager has to be informed immediately in case the ID card is lost.

It is recommended to keep the ID card visible during customer meetings. In the office premises ID card can be held by the employee or kept in a locked space

2.2.5 Cologne, Germany

The building and grounds are monitored by motion detectors, a video surveillance system, and a net-worked building alarm system. A physical access control system is installed at all of the entrances to the building. All of the building's entrance doors are also equipped with a central locking system. Within the building, a digital locking system utilizing transponders and PC recording serves as a system controlling physical access to the offices. Separate code locks secure offices/office areas that

require especially high security. Visitors must register at the reception desk. Visitors are always accompanied by an employee as long as they are on the business premises.

2.2.6 London, United Kingdom

- Visitors must report at the reception or to an employee with which they have an appointment, and are accompanied in the building by an employee.
- The entrance doors are equipped with a digital locking system, opened by employee key cards only. The Office Manager has the list of activated keys used by employees.

2.2.7 New York, USA

- Visitors must report at the reception or to an employee with which they have an appointment, and are accompanied in the building by an employee.
- The entrance doors are equipped with a digital locking system, opened by employee key cards only. The Office Manager has the list of activated keys used by employees.

2.2.8 Houston, USA

- Visitors must report at the reception or to an employee with which they have an appointment, and are accompanied in the building by an employee.
- The entrance doors are equipped with a digital locking system, opened by employee key cards only. The Office Manager has the list of activated keys used by employees.

3. DATA ACCESS CONTROL

This section describes Questback's measures, including identification and authentication, that are in place to prevent unauthorized persons from accessing and using data processing systems, and from accessing and using removable devices.

3.1 Data center

3.1.1 Center in Frankfurt, Germany

Datagroup

The user administration is realized via the Active Directory. In order to grant authorized users exclusive access to the systems and applications relevant for them, DATAGROUP has implemented a comprehensive authorization concept. Access authorizations are assigned according to the need-to-know principle. Employees are thus only granted access to those data whose knowledge is necessary within the scope of the tasks assigned to them. Users are only provided with those applications that they need to perform the tasks assigned to them. The applications are also only assigned the rights necessary to perform the task. On all IT systems, only the user rights required for the specific task are used. Access to system software is blocked for persons who are not administrators. The use of private data media is prohibited by the S2 security policy for employees and administrators. The disposal of data carriers (backup media and hard disks) is always carried out by qualified service providers within the scope of order processing in accordance with Art.28 DSGVO.

Amazon

The Amazon AWS network is accessible to employees, contractors, and any other person required to provide the services in an electronically regulated and controlled manner. AWS maintains access controls and policies to manage access to the AWS network from any network connection and user, including the use of firewalls or functionally equivalent technology and authentication controls. AWS maintains corrective actions and incident response plans to respond to potential security threats.

Oracle

Oracle employees have access to personal data only to the extent necessary to carry out the processing. Oracle imposes confidentiality obligations on employees who have access to personal information. Access to systems by employees (IT staff) is role-based with specially prepared devices. These devices are specially set up and secured by full encryption, firewalls, AntiVirus & AntiSpam. Access is encrypted (SSH, SFTP, SSL) via VPN software with 2-factor authentication. An individual case proof as justification for access is required. Access is via a VDI image or Bastion Hosts. The access is logged (keystroke logging).

3.1.2 Center in North Virginia, USA

AWS has placed a limited number of access points to the cloud in strategic locations to enable more comprehensive monitoring of inbound and outbound communications and network traffic. These customer access points are called API endpoints and provide secure access (HTTPS) that allows you to securely communicate with your storage or data processing instances within AWS. To support customers with FIPS140-2 requirements, Amazon Virtual Private Cloud (VPN) endpoints and SSL terminating load balancers operate in the AWS GovCloud (USA) using FIPS 140-2 Level 2 validated hardware. In addition, AWS has implemented network devices designed to manage interface communications with Internet Service Providers (ISPs). AWS uses a redundant connection to more than one communications service at each point of the AWS network connected to the Internet. Each of these connections has its own network devices.

For more information, visit the AWS Web site at https://aws.amazon.com/security/.

3.1.3 Data center in the Netherlands respectively Ireland

Microsoft's Azure Security has defined requirements for active monitoring. Service teams configure the active monitoring tools in accordance with these requirements. Active monitoring tools include Microsoft Monitoring Agent (MMA) and System Center Operations Manager. These tools are configured to provide real-time alerts to Azure security personnel in situations that require immediate action.

Microsoft provides up-to-date information online:

https://docs.microsoft.com/azure/security/azure-infrastructure-monitoring

3.2 Offices

3.2.1 All offices

All Questback offices will adhere to the requirements in the IT Governance Policy.

Device encryption

All portable storage devices are completely encrypted. (Notebook HDD, USB Sticks)

Authentication

Authentication to the operating system and the applications is by means of individual user IDs and passwords. A separate password must be entered to access the hardware decryption. Employees are required to lock the workplace client whenever they leave the room (“Clear Screen”). Employees also are required to keep their passwords secret and not to divulge them to anybody, even for support purposes. There are password conventions that are implemented technically (system configuration) und organizationally (password policy). According to these conventions, all passwords have to fulfil the defined minimum requirements.

3.3 Software

3.3.1 Enterprise Feedback Suite (EFS)

The standard setting is a follows: The password must be changed after the first login. Thereafter, it expires every 90 days. The licensed software requires users to change their passwords if they login after the expiration date. Account names are not case sensitive. Passwords are case sensitive.

EFS is offering a wide range of password complexity settings:

- Password lengths are variable and determined by the customer.
- Passwords must have at least 6 characters, but no more than 12.
- Passwords must contain characters from at least two of the following four groups: lower case letters (a-z), capital letters (A-Z), numbers (0-9), and other printable ASCII characters. Passwords may not contain spaces.
- Password expiry date, can be set from one day to never expire.
  (Forced password update, validity check of passwords in days)
- Password repeat count, can be set from no count to never use the password again.
  (Check the last x passwords, if the password has been used before)

Users may not employ the same password when they have to change passwords on their first login or after the end of a month. To protect itself against brute-force attacks, the system temporarily blocks access for 30 minutes after six incorrect entries. Passwords are not saved as plain text. Customers can only gain access to and authentication for the licensed software via user-specific accounts.

Rights and role concept of the EFS platform

Power users or administrator accounts are grouped into EFS teams in the Questback platform, which control access to functional rights (ACL) as well as to content rights (objects). If rights / role concepts are to be transferred from external platforms, the concept must first be replicated in Questback EFS. The rights situation can then be mirrored automatically via an API-controlled assignment to the teams in EFS.

Vulnerability Management

Vulnerability scans are conducted using the network and vulnerability scanner Nessus. These scans are conducted for each server once a month. The Nessus default test set is used for these scans. RIPS Code Analysis Scan is used to check the vulnerability of the source code. Security checks can be conducted by the following:

- Questback system administrators (the normal case).
- Customers (at their request and if they bear the costs).
- External security companies (commissioned by a customer who also bears the costs).
- BSI/ISO auditors (during the certification process and when certificates are extended).

Any critical errors that occur are immediately eliminated after the logs have been checked. Data storage media and confidential documents are stored by certified service providers and destroyed in conformity with data protection regulations after the respective purpose no longer applies. The application software EFS records administration accesses in logs. These logs contain information about the account, time, module, action, and other parameters. A separate right is required to inspect the administration log. This right is assigned to specific roles. The standard storage time is 90 days.

3.3.2 Essentials

Customers can only gain access to and authentication for the licensed software via user-specific accounts.

- The password must be changed after the first login
- Account names are not case sensitive
- Passwords are case sensitive
- Passwords must have at least 8 characters, but no more than 20
- Passwords must contain characters from all of the following three groups: lower case letters (a-z), capital letters (A-Z) and numbers (0-9)
- Other printable ASCII characters are accepted, but not required
- Passwords may not contain spaces
- To protect itself against brute-force attacks (10 failed attempts within 30 minute window), the system blocks access to the user account, until opened by Questback support or responsible user in the account
- Passwords are not saved as plain text

3.3.3 QUBIE

Qubie for MS Teams

Users of QUBIE for MS TEAMS can only access and authenticate to the licensed software through their own MS TEAMS accounts. The local authentication conditions of MS TEAMS users apply.

While chatting with QUBIE Bot the Authentication is done by the Bot-Framework / Microsoft Teams and the login for Microsoft Teams is used.

If the user navigates to the new “Results” Tab the OAuth 2 endpoint of Azure Active Directory is used (https://docs.microsoft.com/azure/active-directory/develop/active-directory-v2-protocols). The user has to consent that the account name is shared for the login.

Qubie for Web

The same conditions apply here as for the Enterprise Feedback Suite (EFS).

4. LOGGING OF THE PROCESSING OF PERSONAL DATA

This section describes Questback’s measures for logging and documenting the access to and processing of personal data processed on behalf of its customers.

4.1 Data center

4.1.1 Center in Frankfurt, Germany

Data transmission is logged, and the logs are continuously evaluated. Any removal of data storage media is logged, and the logs are evaluated. Logs and evaluation of logs are performed under the Technical and organizational measures described

herein. Scope of the internet logs: Meta Data of internet traffic. (IP address of the connected client, the called domain, date, time and time zone from which the connection came, the concrete request of the client in plain text, the method used, the requested data, the protocol used, the URL called up, the referrer, the HTTP status code returned on the request, the size of the data transmitted, measured in bytes, operating system and version, type of client, browser and version)

4.1.2 Center in Virginia, USA

Data transmission is logged, and the logs are continuously evaluated. Any removal of data storage media is logged, and the logs are evaluated Logs and evaluation of logs are performed under the Technical and organizational measures described herein. Scope of the internet logs: Meta Data of internet traffic. (IP address of the connected client, the called domain, date, time and time zone from which the connection came, the concrete request of the client in plain text, the method used, the requested data, the protocol used, the URL called up, the referrer, the HTTP status code returned on the request, the size of the data transmitted, measured in bytes, operating system and version, type of client, browser and version)

4.1.3 Data center in the Netherlands respectively Ireland

Microsoft Azure has security mechanisms in place to help manage and monitor Azure cloud services and virtual Azure computers.

Microsoft is responsible for the Azure platform and the physical security of its data centers (through the use of security measures such as electronic access doors, fences and guards). Microsoft Azure provides comprehensive cloud security at the software level that meets its customers' security, privacy and compliance needs.

Microsoft provides security controls and capabilities that support Questback to protect your data and applications.

Microsoft provides the latest information online:

https://docs.microsoft.com/azure/security/security-management-and-monitoring-overview

4.2 Software

4.2.1 EFS

Activities, of both Customers and Questback, are logged in the system. When processing personal data, the software performs a Login Log and an Admin Log. The Login Log informs on which user logged in when, including rejected attempts. Content of the Login Log: Account, IP address, Access/Fail, Error message, Date. The Admin Log provides a detailed log of the actions executed by users in the system. Content of the Admin Log: Entry ID, Account, Lod date, Module name, Action, Execution time, Functions. These logs can be viewed directly in the software. A search and filter function is also offered. A description of the functionalities can be found in the relevant chapters of the software manual.

4.2.2 Essentials

Activities, of both Customers and Questback, are logged in the system. Customer activity is logged to LogActivity and Questback (support/QBAdmin) activity is logged to QBAdmin logs. Content of the LogActivity are ID, TIMESTAMP, LOGGERNAME, MESSAGE, PARAMETERS, SESSIONID, ACCOUNTID, USERID, UPDATEDUSERID, QUESTID, CONTEXTID, EVENTID, TEMPLATEID, RESPONSEID, INVITATIONID, REMINDERID, FOLDERID, REPORTID. Where contextid and eventid describes what the log is about. Content of the QBAdmin logs are: ADMINUSERID, LOGTYPEID, ACCOUNTID, USERID, QUESTID, ID, DESCRIPTION, TIMESTAMP. Where logtypeid describes the log entry. Some of the LogActivity and QBAdmin logs are available in QBAdmin. The software do not offer an UI of these activity logs in the ESS service.

4.2.3 QUBIE

Qubie for MS Teams

MS Teams analytics - Applicationinsights is used to log the different events that can occur within QUBIE.

In QUBIE for MS TEAMS, user activities are logged. This includes events such as error events, question events, role events, feedback events, user events, help events, bug events. The software does not offer a UI of these activity logs.

Qubie for Web

The same conditions apply here as for EFS.

5. TRANSFER CONTROL

This section describes Questback's measures ensuring that personal data cannot be read, copied, changed or deleted during electronic transmission, transport or storage on data storage media and for checking and determining at which points personal data are to be transferred by means of data transmission equipment:

5.1 Data center

5.1.1 Center in Frankfurt, Germany

Encryption of data during transmission ("encryption in transit")

Access to databases at **AWS** and **Oracle** is encrypted and via SSH (Secure Shell) and VPN tunnel. Redundancy is in place for all data lines to the Internet, and they are implemented as BGP (Border Gateway Protocol). The entire network infrastructure (firewalls, switches etc.) has complete redundancy in place. Firewalls and DMZ settings are defined by BSI/ISO standards. Any access by Questback employees (especially from Support or Development) to customer data hosted by the data center for the purpose of administration of the EFS surveys utilizes TLS encryption (PCI compliance). Logging of data transmissions and ongoing evaluation of the logs.

Encryption for resting data ("encryption at rest")

All data in the Frankfurt data centre at **AWS** and **Oracle** are stored in encrypted form when idle.

Written regulations concerning the use of data storage media, including the creation of copies of data storage media for use as backups:

- Such access rights are only granted to administrators
- Any removal of data storage media is logged
- The logs are evaluated

5.1.2 Center in North Virginia, USA

Amazon enables remote employee access via a connection to an AWS access point via HTTPS using a Secure Sockets Layer (SSL), an encryption protocol designed to protect against eavesdropping, data tampering or message forgery. Additional layers of network security are provided by the Amazon Virtual Private Cloud (VPC), which provides a private subnet within the AWS cloud and enables the use of an IPsec Virtual Private Network (VPN) device that can establish an encrypted tunnel between the Amazon VPC and our network. Direct access to customer solutions over a remote connection is not allowed. There is a policy to maintain security throughout the remote access provisioning process and to address security issues during teleworking. The process includes two-factor authentication (RSA+PIN and SSO) and a bastion server. Access to the databases is encrypted via SSH (Secure Shell) and VPN tunnel. All data lines to the Internet are redundant and designed as BGP (Border Gateway Protocol). The entire network infrastructure (firewalls, switches, etc.) is completely redundant. Firewalls and DMZ settings are defined by ISO standards. All data exports are logged in the licensed software. Any access by Questback employees (especially from support or development) to customer data hosted by the data center for the purpose of managing EFS surveys is done using TLS encryption (PCI compliance). Logging of data transmissions and ongoing evaluation of the logs. Written policies on the use of media, including the making of copies of media for use as backup.

5.1.3 Data center in the Netherlands respectively Ireland

Encryption for dormant data

Dormant data includes information stored in any digital format in permanent storage on physical media. Media includes files on magnetic or optical media, archived data, and backups. Microsoft Azure offers a range of data storage solutions for a variety of needs, including file, data, blob, and table storage. Microsoft also provides encryption to protect Azure SQL Database, Azure Cosmos DB, and Azure Data Lake.

Data at rest encryption is available for services in all Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), and Infrastructure-as-a-Service (IaaS) cloud models. This article summarizes and provides resources to help you take advantage of Azure's encryption options.

For a detailed discussion of Azure dormant data encryption, see Azure dormant data encryption.

Encrypting Data During Transmission

Microsoft Azure provides many ways to protect data as it is transferred between different locations.

TLS/SSL Encryption in Azure

Microsoft uses the Transport Layer Security Protocol (TLS) to protect data as it moves between cloud services and customers. Microsoft data centers negotiate a TLS connection with client systems that connect to Azure services. TLS provides rigorous

authentication, message privacy and integrity (enabling detection of message tampering, interception, and forgery), interoperability, algorithm flexibility, and ease of deployment and use.

Perfect Forward Secrecy (PFS) protects connections between customers' client systems and Microsoft cloud services with unique keys. The connections also use RSA-based encryption key lengths of 2,048 bits. This combination makes it difficult to intercept and access data during transmission.

Microsoft provides up-to-date information online:

https://docs.microsoft.com/azure/security/security-azure-encryption-overview

5.2 Offices and Software

Data access to all the software components of the survey platform can be provided using TLS encryption. The transmission of personal data is secured by the use of HTTPS/TLS encryption. To this end, Questback provides a data transfer platform in projects. The type and scope of the data transferred (metadata) is logged. These logs are regularly evaluated. The use of mobile data storage media is basically forbidden. The use of mobile storage media is permitted for certain data subject to advance written approval. However, personal or security-relevant information does not belong to this category. All mobile workstation computers are completely encrypted. Email communication and access to documents from the contractor's employees are protected by encryption, VPNs, and firewalls.

6. INPUT CONTROL

This section describes Questback's measures ensuring that whether and by whom personal data has been entered, changed or deleted in the data processing systems can be checked and determined:

6.1 Data center

6.1.1 Center in Frankfurt, Germany

The employees of the data center of DATAGROUP, Amazon and Oracle, who are responsible for remote maintenance measures can neither enter data into the data processing systems nor view, change nor delete personal data of Questback customers. Remote maintenance measures are logged by a firewall. The resulting logs are checked randomly (spot-checks) and whenever warranted by events.

6.1.2 Center in North Virginia, USA

The employees of the data center of Amazon, who are responsible for remote maintenance measures can neither enter data into the data processing systems nor view, change nor delete personal data of Questback customers. Remote maintenance measures are logged by a firewall. The resulting logs are checked randomly (spot-checks) and whenever warranted by events.

6.1.3 Data center in the Netherlands respectively Ireland

Microsoft's data center personnel responsible for maintenance cannot enter data into data processing systems or view, modify, or delete personal information about Questback customers. Remote maintenance is logged through a firewall. The resulting logs are checked on a random basis and whenever events warrant it.

6.2 Offices

All Questback offices will adhere to the requirements in the IT Governance Policy, hereunder definition of security zones. The following sections describe specific elements in place for each office.

All employees sign a confidentiality clause as an integral part of their employment contracts, hereunder a commitment to maintaining data secrecy, which protects clients even after the employees' job contracts are terminated or expire. A ticket system in the support and administration area ensures that all tasks are completed correctly and on time. The contractor's employees are supported by a directory service and may only access such data as is needed for their work within the framework of the respective task area and field of activity.

6.3 Software

6.3.1 EFS

All changes to version statuses are documented. Use is documented with regard to the respective account; the associated data is stored for a maximum of 90 days. During the use of the exchange platform, files containing personal data are stored by version. The associated date, time, and user are logged. User remarks can be entered into a commentary field that is not included in the document. Documents cannot be changed. Documents that are entered into the system can be provided with a separate password protection in order to restrict access.

6.3.2 Essentials

All activity in the system is stored in an Activity Log in the database. The associated date, time, user and activity is logged. This log is never deleted.

6.3.3 QUBIE

Qubie for MS Teams

In QUBIE for MS TEAMS the events a user can trigger are logged into application insights. More details see 4.2.3.

Qubie for Web

The same conditions apply here as for EFS.

7. ASSIGNMENT CONTROL

This section describes Questback's measures ensuring that personal data which are processed on behalf of a client can only be processed in accordance with the client's instructions.

7.1 Data center

Questback will audit the respective security concepts and inspect the data center premises. Written contracts with the Data Centers are in place to ensure the maintaining of data protection.

At no time do the cloud providers Datagroup, Microsoft, Amazon or Oracle process personal data without a contract. All employees are subject to confidentiality agreements (NDAs).

7.2 Offices

All Questback employees adhere to Questback Binding Corporate rules, and receive regular training on how to protect personal data. The assessment of content in any Data Processing Agreement, or in instructions from client are part of such training.

Questback managers, and Questback employees who are in dialogue with customers, are under obligation to ensure that instructions are provided to relevant personnel, and adhered to.

7.3 Software

When a customer's subscription to any of Questback's services is terminated or expired, the account will be deactivated and becomes non-accessible. Information collected through the site will be deleted.

8. CONFIDENTIALITY CONTROL

The GDPR section 32 defines confidentiality control as a requirement to ensure security of processing. This section describes Questback's measures ensuring confidentiality control.

8.1 Data Center

Questback's data centers, which are responsible for the storage and technical operation of the data, have no access to the data. The operators of data centers do not have an account on Questback's servers. Exceptions to this rule apply only to the creation of backups so that the backup software can back up the data. The backups are stored securely and documented and are subject to strict access rules. Backups are stored in encrypted form.

Questback HQ
Bogstadveien 54
0366 Oslo
NORWAY

8.2 Offices

Questback offices ensures confidentiality through a variety of measures. This includes visitor management, room locking system, strong account management, clean workplace rules, encrypted devices, confidentiality agreements, sealed stored backup media and certified destruction of data media.

8.3 Software

Questback's software ensures confidentiality through a variety of measures. This includes access through strong account management, use of certified data center, 2nd factor access control, privacy data tagging and encrypted transport over internet.

9. INTEGRITY CONTROL

The GDPR section 32 defines integrity control as a requirement to ensure security of processing. This section describes Questback's measures ensuring integrity control.

9.1 Data Center

Questback's data centers ensure integrity through a variety of measures. These include various national and international certifications, such as ISO27001 or SOC, which in their form maintain the integrity of all information processing systems and data, as well as encrypted backup tapes and encrypted transport over the Internet.

9.2 Offices

Questback offices ensure integrity through a variety of measures. This includes encryption of media, strong access controls, use of encrypted communication and encapsulated network segments.

9.3 Software

Questback's software ensures integrity through a variety of measures. This includes ensuring of the integrity of the program modules via (crypt.) checksums/comparison against reference list, URL manipulation mechanisms, secure cookies, specific Web service rights and logging, secure sandbox programming extension LUA, continuous improvement of current codebase, file integrity checks, change audit log and input validation controls.

10. AVAILABILITY CONTROL

The GDPR section 32 defines availability control as a requirement to ensure security of processing. This section describes Questback's measures ensuring that personal data is available, while preventing that it is not accidentally destroyed or lost, hereunder routines for backup and recovery.

10.1 Data center

10.1.1 Center in Frankfurt, Germany

Each of our cloud providers (Datagroup, Amazon, Microsoft and Oracle) perform complete daily backups of the data. Thanks to this backup, the contractor can immediately resume operations in case of an emergency. The data is copied in parallel to a separate backup system in a separate fire compartment. The data is also copied to magnetic tapes, which are stored separately and securely. The data on the magnetic tapes is encrypted on a case-by-case basis. The log files of the data backup are checked daily.

Every week, all the backups of the central server are placed in a secure cabinet. The backups for each day of the previous eight weeks can be precisely restored. Regular training of data recovery and data readability checks are carried out as part of emergency drills.

- Climate control: Four independently operating air conditioning systems are installed.
- Fire protection: The computer rooms are equipped with a fire detection system that is connected to the fire department and an argon fire extinguishing system.
- Power supply: An emergency power system (uninterruptible power supply) is installed.
- Redundancy is in place for all systems.
- Up-to-date written guidelines and/or work instructions exist.

10.1.2 Center in North Virginia, USA

Availability

The Amazon data centers will be built in clusters in different regions of the world. In the event of a failure, automatic processes shift customer data traffic away from the affected areas. The core applications are deployed in an N+1 configuration so that in the event of a data center failure, there is sufficient capacity to distribute the traffic load to the remaining sites. AWS places instances and stores data within multiple geographic regions and across multiple availability zones within each region. Each Availability Zone is designed as an independent failure zone. This means that Availability Zones are physically distributed within a typical urban region, e.g. in areas with lower flood risk (flood zone categorizations vary by region). In addition to a stand-alone uninterruptible power supply and on-site emergency power generators, all Availability Zones are supplied by independent power suppliers over different power grids to minimize single fault locations. All Availability Zones are redundantly connected to multiple Tier 1 transit providers. Amazon manages incidents through industry-standard diagnostic procedures to drive the resolution of mission-critical incidents.

AWS operations staff provide 24/7, 365-days a year continuous staffing to identify incidents and manage their impact and resolution. The members of the Board of Directors' Management and Audit Committee regularly review the stability plans of AWS Services. Amazon reviews the availability of the customer solution from a network and hardware availability perspective as well as the availability of support services and regularly reviews controls, processes and architectures to ensure the best possible availability.

This includes documented guidelines that follow the recommendations of standards (such as ISO27001) (including an information security policy); a formal capacity management process to ensure the availability of all resources required by the organization, including bandwidth, data center capacity and utilities, inventory and workforce, and employee skills; uninterruptible power supplies (UPS) to minimize the risk of short-term power outages and fluctuations; diesel generators to minimize the risk of long-term power outages and fluctuations; data center roofs and exterior walls designed to withstand heavy loads and extreme weather conditions, including Light protection; temperature and humidity climate systems in the storage area as well as equipment with fire alarm and extinguishing systems, fire extinguishers.

Backup and Restore

The AWS Backup Process is a fully managed backup service that centralizes and automates data protection across AWS services using AWS Storage Gateways. Backup policies are centrally configured and resources for backup activity are permanently monitored. AWS Backup is automated and consolidates backup tasks to avoid custom scripts and manual processes. Backup policies define the automation of backup schedules and retention of backups. The backup process is structured to meet the needs and requirements of the organization. The default schedule is weekly full and daily differential backups with retention rates of eight weeks.

AWS Backup protects the backups by encrypting the data at rest and during transmission. The backup activity logs are available for compliance checks. AWS Backup is PCI, ISO and HIPAA compliant.

10.1.3 Data center in the Netherlands respectively Ireland

Microsoft Azure provides reliable availability based on comprehensive redundancy using virtualization technology. Microsoft Azure provides multiple levels of redundancy to ensure maximum availability of customer data.

The Microsoft Cloud Infrastructure and Operations team designs, builds, operates and enhances the protection of cloud infrastructure. This team ensures high availability and reliability, high efficiency, intelligent scalability for the Azure infrastructure. The team provides a more secure, private and trusted cloud.

Uninterruptible power supplies and huge battery banks ensure continued power supply in the event of short-term power outages. Emergency generators provide backup power during extended downtime and scheduled maintenance. In the event of a natural disaster, the data center can use the on-site fuel reserves.

Stable high-speed fiber optic networks connect data centers to other major hubs and Internet users. Server nodes host workloads closer to the user to reduce latency, provide georedundancy, and increase overall service resilience. A team of technicians works around the clock to ensure that services are always available.

Microsoft ensures high availability through advanced incident monitoring and response, service support, backup, and failover. Geographically dispersed Microsoft operations centers operate 24 hours a day, 7 days a week, 365 days a year. The Azure network is one of the largest in the world. The fiber optic content distribution network connects data centers and edge nodes to ensure high performance and reliability.

Azure SQL Server databases are automatically backuped (https://docs.microsoft.com/azure/sql-database/sql-database-automated-backups) Full database backups are created every 12 hours, transactional backups are created every 5-10 minutes.

Microsoft provides up-to-date information online:

https://docs.microsoft.com/azure/security/azure-infrastructure-availability

Questback HQ
Bogstadveien 54
0366 Oslo
NORWAY

10.2 Offices

Backup strategy:

- Every night, a complete backup of the data is made on an independent backup system. Thanks to this backup, the contractor can immediately commence operations again in the event of an emergency.
- Every week, all the backups of the central server are placed in a safe.
- Backups can be precisely restored for each of the previous seven to 30 days depending on how critical the system is.

Additional measures:

- The computer rooms are equipped with climate control.
- Power supply: An emergency power system (uninterruptible power supply) is installed.
- Certified fire extinguishers are available.
- Antivirus protection, spam filters, and firewalls are used.

10.3 Software

Backup strategy:

- Every night, a complete backup of the data is made on an independent backup system. Thanks to this backup, the contractor can immediately commence operations again in the event of an emergency.
- Every week, all the backups of the central server are placed in a safe.
- Backups can be precisely restored for each of the previous seven to 60 days depending on how critical the system is.

11. RESILIENCE OF PROCESSING SYSTEMS AND SERVICES

The GDPR section 32 defines resilience of processing systems and services as a requirement to ensure security of processing. This section describes Questback's measures ensuring resilience of processing systems and services.

11.1 Data Center

Questback's Data Center ensure resilience through a variety of measures. This includes use of scalable network components, on the fly connectable resources, fault-tolerant hardware components, state of the art network infrastructure, provision of sufficient personnel and permanent monitoring of operational health.

11.2 Offices

Questback's offices ensure resilience through a variety of measures. This includes use of scalable network components, forward-looking planning of needs, provision of sufficient personnel and permanent monitoring of operational health.

11.3 Software

Questback's software ensure resilience through a variety of measures. This includes use Scalable database, modern coding, agile development, use of high performance software components.

12. SEPARATION RULE

This section describes Questback's measures ensuring that data that has been collected for different purposes is processed separately.

12.1 Software

12.1.1 EFS

Segregation of personal data at different storage areas by means of organizational and physical separation (multi-client capability). The data processing systems for especially sensitive data are separated physically and organizationally. Test computers are physically separated from live systems and are subject to separate security restrictions. Mirrors of the live system are created for test purposes whenever installations are altered. All personal data is anonymized before tests are conducted.

12.1.2 Essentials

Segregation of personal data is done logical by ID filtering via code (multi-client capability). The data processing systems for especially sensitive data are separated physically and organizationally. Test computers are physically separated from live

systems and are subject to separate security restrictions. Separate environments for staging and penetration testing are in place for test purposes whenever installations are altered. All personal data is anonymized before tests are conducted.

12.1.3 QUBIE

Qubie for MS Teams

In QUBIE for MS TEAMS the personal data is logically separated by ID filtering (multi-client capability). Data from different mandates is logically separated in the databases. Test instances are separated from live systems and are subject to separate security restrictions. Separate instances for staging and penetration testing are available for testing purposes. All personal data is anonymized prior to testing.

Qubie for Web

The same conditions apply here as for EFS.

13. PSEUDONYMISATION AND ENCRYPTION OF PERSONAL DATA

The GDPR section 32 defines pseudonymisation and encryption of data as a requirement to ensure security of processing. This section describes Questback's measures ensuring pseudonymisation and encryption of data.

13.1 Data Center

Questback's Data Center communicate encrypted with customers, using modern transport encryption. Backups are stored case-dependent encrypted.

13.2 Software

Questback's software store passwords encrypted (hashed). The data are anonymized in the system by means of a script. All data fields (such as email address, first name / surname) are replaced by generic information. (Overridden by the script in the database).

14. RETENTION AND DELETION

This section describes Questback's retention time for data, hereunder personal data, processed by Questback on behalf of its customers. Furthermore, the routines for deletion of data is defined.

14.1 Data center

The data centers retain the data for the duration of an existing contractual relationship between Questback and its customers. After a customer contract ends, Questback terminates the customer installation and database.

14.2 Software

14.2.1 Default setting: retention time for personal data defined by Questback's customer

Questback software is made available for Questback's customers, for them to create surveys and questionnaires that are made available for respondents. Upon creation of survey or questionnaire, customer will define retention time for the data in question. The data will be anonymized automatically when the retention time has passed. Data stored in back-up will be deleted (over-written) no later than 60 days after the original data has been deleted. Deletion will take place in accordance with Questback then-current deletion routines.

14.2.2 Optional setting: retention time not defined by customer

Should customer not choose to define retention time, the data in question will be kept until deleted manually, or until the contract between Questback and Customer is terminated. Data stored in back-up will be deleted (over-written) no later than 60 days after the original data has been deleted. Deletion will take place in accordance with Questback then-current deletion routines.

14.2.3 QUBIE

Qubie for MS Teams

Questback HQ
Bogstadveien 54
0366 Oslo
NORWAY

QUBIE for MS TEAMS stores data for the duration of the use of the app. The data is irretrievably deleted when the app is uninstalled.

Qubie for Web

The same conditions apply here as for the Questback software standard and optional settings.

15. INCIDENT MANAGEMENT

Breach notification is a mandatory topic between Questback and its customers. A data breach which result in a risk for the rights and freedoms of individuals will be handled according to applicable law. Breach notification must be done within 72 hours of first having become aware of the breach. Questback will notify our customers, the controllers, "without undue delay" after Questback first became aware of a data breach.

While the above statement only indicates the requirement for notification within 72 hours of identifying a data breach and does not say Questback must have an incident response program, it is evident that to meet the 72-hour notification requirement, Questback provides to be in a position to quickly detect a breach within their networks, systems, or applications.

15.1 Detection

To be able to detect an attack or security event, Questback has established several monitoring and control measures which alert in case of an attack. Questback then immediately take action against an adversary within the network, especially if an early detection opens the possibility to stop the attack before he can do any damage.

Questback's response framework gives the ability to quickly analyse what the attackers may have accessed or copied. This will go a long way in minimizing the potential impact to the customer and, most importantly, to the individuals that were impacted.

15.2 Communication

Beside the detection requirements identified above, internal communication between impacted departments and groups was agreed as well, to ensure a smooth response to an incident or breach. A communication plan identify who is authorized to talk to external entities and customers.

Questback routinely test the response program to ensure effectiveness and timely notification, to comply with regulatory requirements and timeframes.

15.3 Notification

To reduce the risk of not having a complete or thorough response, Questback has developed an incident response program, created policies and procedures, and ensured everyone is aware of the program.

Questback's data inventory helps to know where an individual's data is being stored, so the incident response team quickly know the potential impact of a security event on a system or application. Questback's accurate inventory of data is crucial to help with any potential individual notifications in the event of a breach, by pointing to which customer is impacted and support the process to notify the customer in the event of a breach. The then starting communication with the customer describe the nature of the breach and recommendations to mitigate potential adverse effects.

16. INTERNAL CONTROL

This section describes Questback's measures ensuring that its policies, including the policies described in this document, are adhered to through the organization, and the process for regularly testing, assessing and evaluating the effectiveness of these technical and organisational measures.

16.1 Monitoring

16.1.1 EFS & Essentials

- Questback monitors more than 1000 hosts and more than 4500 services of dedicated and shared instances
- Every minute, about 1000 checks are executed and reported
- Alerts are issued 24x7
- Alerts are immediately picked up by Questback's experienced system administrators
- The monitoring system has redundancy in place and is observed by a third party monitoring tool
- A further fourth monitoring system gives insights to the platforms' performance from places all over the world

Questback HQ
Bogstadveien 54
0366 Oslo
NORWAY

16.2 Security Audits

Regular audits of the hosting environment are part of the ISO 27001 certificate requirements.

Apart from the ISO audit, Questback has been subject to various ad-hoc audits performed by some of our customers who require verification for the highest security compliance. Questback also performs frequent self-audits.

16.2.1 Security Audit

To comply with the high requirement towards the platforms' security, as well as ISO 27001 certification requirements, Questback hires 3rd party security experts to conduct security tests towards our platforms. The aim is to ensure continuous security when it comes to current and up-and-coming technologies and constant incremental development work.

The tests are conducted as an application test with focus on the following areas:

- OWASP Top 10
- Cross-Site scripting (XSS)
- Session Fixation
- Weak or missing authentication
- Hidden parameters
- Directory browsing
- SQL Injection

16.2.2 Regularity of Security Audits

- 1 - 2 application tests of the service are performed every year
- 1 Infrastructure test of our hosting environment each year – this is covered in more detail in hosting section.

16.2.3 Results of Audits

- Results of application and infrastructure tests are presented to Product Management
- Any critical vulnerability is sent to development to be fixed
- Operation department takes care of issues related to infrastructure and server environment
- Issues related to Questback server environment are fixed by IT operations
- Vulnerabilities in commercial website www.questback.com are fixed by developers responsible for the design of our front-end webpages