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: 1.35
Approved on: July 03th, 2018
Approved by: Eric M. Roßner and Sara Habberstad

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 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 two separate software platforms: Enterprise Feedback Suite (EFS) and Essentials.

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[1]. 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 or Rackspace data centers.

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[2] (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, 2018; this certificate is available upon request)

Processing in software platforms in the Data Center in 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 Rackspace. Rackspace has been certified as follows:

- In accordance with to ISO/IEC 27001:2013 (certificate number: IS 636168, valid until October 20th, 2018; this certificate is available upon request)

In addition, confirmation letters for compliance with 2015 SSAE 16 / ISAE 3402 Type II SOC 1, and Type II SOC 2 and SOC 3 can be provided upon request.

[1] Essentials is provided from Data Center in Germany only

[2] The IT-Grundschutz Certificate is a German self-declaration that offers companies the possibility to make their efforts regarding IT security transparent.

Questback HQ
Bogstadveien 54
0366 Oslo
NORWAY

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
Rackspace Limited	5 Millington Road, Hyde Park Hayes, Middlesex UB3 4AZ	UK
Rackspace Limited (Rackspace Ashburn DataCenter)	44480 Hastings Drive, Ashburn, VA 20147	Virginia, USA
Rackspace Limited (Rackspace Dallas DataCenter)	801 Industrial Boulevard, Grapevine, TX 76051	Texas, USA

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	295 Madison Avenue, 45th Floor New York, NY 10017	New York, USA
Questback, Inc.	21 Waterway Avenue #500 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.

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 that is connected to the police. The data center is located on the second floor and has two separate access control mechanisms. Video surveillance is used to monitor the computer room. In accordance with ISO27001, DATAGROUP Bremen GmbH has a physical access authorization concept ("BSI Zertifizierung-, Documentation-, Berechtigungskonzept für Gebäude"), which is available for inspection on site. A two-stage access system has been installed to control physical access to the high-security areas of the data center. Physical access is arranged on application by the team leader and cross-checking by the management of DATAGROUP Bremen GmbH. This physical access is set up on a corresponding transponder for the employee in question. In the second stage of the data center's physical access concept, code locks are added for the data center administrator group "Wissen". The physical access authorization lists are repeatedly checked and updated during internal and external ISO27001 audits immediately whenever there are any changes to the physical access authorizations.

2.1.2 Center in 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. Rackspace 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.

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

Excerpt from the DATAGROUP security guideline "S2 für Mitarbeiter und Administratoren: Zugangs- und Zugriffskontrolle" (available for inspection on site at DATAGROUP Frankfurt):

The administrator is responsible for setting up, documenting, and preventing manipulation of the data access and usage rights and of any changes to them. The administrator must always employ the data access rights that are appropriate to his respective role when using the system (separation of administrator and user rights). In accordance with DATAGROUP IT Service Management, changes are documented in line with the change process using the documentation tool Magic Service Desk. Access to the functions of information and application systems is restricted in accordance with a role-based authorization group access. A secure login system activated via a group policy of the DATAGROUP Active Directory is used to control data access to the systems and applications. An interactive password management system is accordingly used. The main additional technical measure for protection against data manipulation is encryption. The corresponding specification ("BSI Zertifizierung-Kryptokonzept") can be inspected on site at DATAGROUP Frankfurt. The integrity of the system software is ensured by a checksum comparison.

3.1.2 Center in Virginia, USA

Rackspace secures access to core networking infrastructure utilizing inherent access control functionality in TACACS+ software. TACACS+ is an industry standard network device access control system. Processes are in place to review the TACACS+ access lists on a quarterly basis to verify those users on the list still require access. Any discrepancies found are corrected immediately. Access to network devices via TACACS+ is initially provisioned only to those employees that require it on a role specific basis and are able to pass both a written and lab examination. Rackspace is responsible for the logging and monitoring of Rackspace employee access to the customer solution on bastion servers. These servers help protect the customer environment by logging all employee activity in the customer environment. All other customer specific logs, including server and firewall logs, are the responsibility of the customer. Rackspace can provision an Alert Logic Log Manager device into the customer solution if required. Alternatively, the customer can install and configure their own log management solution, such as the operation of a sys-log server. Rackspace maintains an internal Access Control Policy in accordance to ISO27001 requirements. The access control policy defines procedures for the creation of new Rackspace user accounts and addition of initial privileges and rights, change and removal of Rackspace user privileges and termination of Rackspace user accounts. As the primary system administrator, the customer is responsible for the management of any non-Rackspace user accounts, including creation, change management and termination, and enforcement of related remote working and password controls.

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:

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

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)

4.2 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.

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

Access to databases 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 SSL encryption (PCI compliance). Logging of data transmissions and ongoing evaluation of the logs. 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 Virginia, USA

Rackspace allows remote employee access through VPN authentication which requires two-factor authentication using RSA token and password. Direct access to customer solutions via remote connection is not permitted. A policy is in place to maintain security throughout the remote access provisioning process and to manage security concerns while teleworking. The process involves two-factor authentication (RSA+PIN and SSO) and a bastion server. Access to databases 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 ISO standards. Any exports of data 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 administration of the EFS surveys utilizes SSL encryption (PCI compliance). Logging of data transmissions and ongoing evaluation of the logs. Written regulations concerning the use of data storage media, including the creation of copies of data storage media for use as backups.

5.2 Offices and Software

Data access to all the software components of the survey platform can be provided using SSL encryption. The transmission of personal data is secured by the use of HTTPS/SSL 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 Frankfurt, 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 Virginia, USA

The employees of the data center of Rackspace, 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.

6.2 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.

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.

Questback HQ
Bogstadveien 54
0366 Oslo
NORWAY

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 Center, which are applied to store and technically host the processing of the privacy data, do not have access to the privacy data. The data center operators 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 secure and documented stored in encrypted form and are subject to strict access rules.

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 Center ensure integrity through a variety of measures. This includes use of 27001/SOC certified data center which maintaining the integrity of all IT systems and data as part of the certification controls, encrypted backup tapes, and encrypted transport over 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.

Questback HQ
Bogstadveien 54
0366 Oslo
NORWAY

10.1 Data center

10.1.1 Center in Frankfurt, Germany

Every night, a complete backup of the data is made on an independent hard disc within the server employed. Thanks to this backup, the contractor can immediately commence operations again in the event of an emergency. Every night, the data is copied onto a separate backup system located in a separate fire area. The data is also copied onto magnetic tapes that are stored in a bank safe. The data on the magnetic tapes is encrypted. Every day, DATAGROUP administrators check the data backup log files.

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 Virginia, USA

The Rackspace Managed Backup (MBU) is a shared backup infrastructure designed to provide data storage and protection. Servers are backed up to our centralized Managed Backup Storage System. The backup process is structured to meet business needs and requests. The default schedule is Weekly Full and Daily Differential backups with retention rates of two or four weeks.

Managed Backup utilizes an independent private network for backups running on network equipment. This was done to minimize network security concerns with the following results:

- Each server is in a port level VLAN.
- Each customer's server can only see the backup servers and no other servers on the network, including their own.
- No customer can see any other customer's server on another port level VLAN.

To support a wide range of Managed Backup capabilities, Rackspace currently leverages a number of infrastructure components including CommVault software on Data Domain disk technologies and/or LTO tape technologies within Quantum/ADIC and Sun libraries.

Rackspace considers the availability of the customer solution from the perspective of network and hardware uptime and the availability of our support services to be of the highest importance, and regularly reviews controls, processes, and architecture to help provide the best available uptime.

- Documented policies which meet the recommendations of the ISO27001 standard (including an Information Security Policy).
- Formal capacity management process to help ensure the availability of all resources required by the business including bandwidth, data center capacity and utilities, inventory and employee manpower and skills.
- Uninterruptible power supplies (UPS) to mitigate the risk of short-term utility power failures and fluctuations.
- Diesel generators to mitigate the risk of long-term utility power failures and fluctuations.
- Data Center roofs and exterior walls of are heavy duty rated and are designed to withstand extreme weather. Appropriate lighting protection is fitted.
- Temperature and humidity climate control systems within the vault area
- Data centers are equipped with fire detection and suppression systems, fire extinguishers.

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.

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 encrypted.

Questback HQ
Bogstadveien 54
0366 Oslo
NORWAY

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

Data Centres will retain data for the duration defined by Questback. 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.

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

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

Questback HQ
Bogstadveien 54
0366 Oslo
NORWAY

17.DOCUMENT HISTORY

Author:	Version:	Revision	Date:	Approved by:
Questback IT Operations	1	Translation of Technical and Organizational measures from the German document applicable only to Questback GmbH, EFS and DATAGROUP.		Thorsten Grote
Sara Habberstad Eric M. Roßner	1.1	Language revision, addition of sections and content for all offices, both Data Centers and both software platforms	08AUG17	Sara Habberstad
Eric M. Roßner	1.2	Small additions regarding ESS controls and measures	16OCT17	Eric M. Roßner
Eric M. Roßner	1.21	Changing Datagroup Bremen Address	30JAN18	Eric M. Roßner
Eric M. Roßner	1.22	Changing EFS password complexity and forced PW change (Chapter 3.3.1)	08MAR18	Eric M. Roßner
Sara Habberstad Eric M. Roßner	1.31	Updates to meet increased request for descriptions on a detailed level: Added sections 1.4, 4, 8, 9, 11, 13 14 and 15. Added Appendix 1.	27APR18	Eric M. Roßner, Sara Habberstad
Eric M. Roßner	1.32	Small changes in 10.1.1, Tape storage and encryption	04MAY18	Eric M. Roßner
Eric M. Roßner	1.33	Typo in 1.2, Country Rackspace Limited	06JUNE18	Eric M. Roßner
Eric M. Roßner	1.34	Small changes in 10.2 & 10.3, backup retention time	20JUN18	Eric M. Roßner
Eric M. Roßner	1.35	Small changes in 1.2, recent certificates	03JUL18	Eric M. Roßner

Questback HQ
Bogstadveien 54
0366 Oslo
NORWAY

18. APPENDIX 1 FAQ

Frequently asked questions related to Questback Technical and organizational measures.

Date: April 27th, 2018.

TOPIC	QUESTION	Questback answer
Volume of personal data processed	How many individual records does Questback hold for a customer?	Questback provides a tool for its customers to collect and assess feedback. The customer is in full control with how many individuals are invited to surveys, and the volume of data collected per survey.
Data Retention	How long does Questback retain personal data records?	When Questback customers create a survey, the retention time for personal data is defined by customer. When the defined retention time is over, personal data is automatically deleted in accordance with Questback deletion routines.
Types of data	What personal data does Questback process on behalf of its customers?	Questback provides a tool for its customers to collect and assess feedback. The customer decides which types of personal data it collects from respondents. Typical types of personal data processed are e-mail address, IP address, name and age. Customer employees who use software (Users) provide their name and e-mail address, and may also provide other information relevant for their use of the software.
	What special categories of data (sensitive data" does Questback hold or process?	Questback provides a tool for its customers to collect and assess feedback. The customer is in full control with the types of personal data collected. Customer is free to add sensitive data.
ACCESS	Who can access personal data from respondents within Questback's organization?	Data in Questback software is accessed by the following: • Customer's users • Questback support personnel, for the purpose of providing support • If relevant under contract with customer, Questback consultants • A list of access is provided in annex to Questback Data Processing Agreement
	Who can access personal data from respondents outside Questback's organization?	Questback's Hosting provider in Germany manages the ISO certified server environment in accordance with ISO27001. If specifically agreed in contract with Customer, a sub-processor defined in such contract may be given access rights.

Questback HQ
Bogstadveien 54
0366 Oslo
NORWAY

TOPIC	QUESTION	Questback answer
Subcontractors	Does Questback subcontract any of the services it provides to customers?	A full list of subcontractors is provided in annex to Questback Data Processing Agreement, and includes Hosting provider and Questback entities in the EEA.
	Does Questback have a GDPR compliant sub-processing agreement in place with its sub-processors?	Yes
DATA STORAGE / SECURITY	Where does Questback store/host data.	Personal data from Questback's customers located in the European Economic Area (EEA) is stored in data halls in Frankfurt, Germany
	Are any services provided outside the European Economic Area (EEA)?	If no specific agreement is in place with customer, no personal data will be processed outside the EEA. If agreed in contract with customer, and with appropriate safeguards as defined in the GDPR in place, support or consulting services may be provided from outside the EEA.
	Is data transferred outside the European Economic Area (EEA)?	No personal data is transferred outside the European Economic Area, unless specific agreement is in place with customer, and Safeguards that are defined as appropriate under GDPR are in place
	How is data from different customers segregated from each other?	EFS: Customer Data is segregated in databases (often referred to as "instances"), each customer has his own dedicated database. Essentials: Segregation of personal data is done logical by ID filtering via code (multi-client capability).
	Is access restricted to specific personnel?	Only Questback's Systems Engineering department located in Cologne, Germany, has access. The access is reviewed by Questback's ISO 27001 BSI certified data centre regularly. Each member of the Systems Engineering team has an individual VPN account to access the network, in addition to using their own accounts and root account to access data.
	What controls are in place to ensure data has not been accessed, manipulated or extracted unless required for a particular task?	Questback uses database audit logging to monitor any data or schema access and changes.
	Are independent reviews performed to ensure adherence to the information security policies and requirements?	External vulnerability tests are performed at least annually

Questback HQ
Bogstadveien 54
0366 Oslo
NORWAY

TOPIC	QUESTION	Questback answer
	Will personal data be stored on portable media?	No. Note, however, that consultants may process personal data locally as part of specific projects required by customer from time to time. Such personal data is deleted once the agreed project or task is fulfilled.
	Does your organization have a dedicated data security team?	Yes, the team is located in our offices in Cologne, Germany.
The data subjects' rights	How does Questback ensure that the data subject's right to access its data is fulfilled	A User (customer employee) who wishes to access his or her user access data, is free to do so at any time. A respondent who wishes to access his or her data, will be directed to customer (the controller). Currently, Questback will provide data related to such individuals upon request from customer, and Customer will be able to provide to Respondent. Respondent will not be able to access or affect the fulfilled survey itself.
	How does Questback ensure that the data subject's right to rectification is fulfilled	A User (customer employee) who wishes to rectify his or her user access data, is free to do so at any time. A respondent who wishes its data to be rectified, will be directed to customer (the controller). Controller will assess if rectification or deletion is relevant, as rectification in ongoing surveys may not be an option. Currently, Questback will perform deletion or rectification of such individuals upon request from customer. Future release will give customer access to perform such rectification itself.
	How does Questback ensure that the data subject's right to erasure is fulfilled	A User (customer employee) who wishes to erase his or her user access data, is free to do so at any time. A respondent who wishes to be deleted, will be directed to customer (the controller). Currently, Questback will perform deletion of such individuals upon request from customer. Future release will give customer access to perform such deletion itself.
	How does Questback ensure that the data subject's right to restriction of processing is fulfilled	For the purpose of surveys, restriction of processing will in practice mean that personal data must be deleted from the survey. If this is not the case, the personal data will continue to be processed. Questbacks answer related to deletion will therefore be relevant
	How does Questback ensure that the data subject's right to data portability is fulfilled	For the purpose of surveys, data portability will in practice mean that a respondent will have the possibility to receive access his data in machine readable format. A respondent who wishes its data, will be directed to customer (the controller). Currently, Questback will provide overview related to individual data subjects upon request from customer.

Questback HQ
Bogstadveien 54
0366 Oslo
NORWAY

TOPIC	QUESTION	Questback answer
	How does Questback ensure that the data subject's right to objections to processing is fulfilled	Respondents to surveys will be given contact information to the controller, and information that they can contact controller if they wish to withdraw consent. A survey, when completed by respondent, will no longer be something that the respondent has access to. It is therefore not possible to withdraw consent in the survey itself.
	How does Questback manage the data subjects' rights related to automated decision making and profiling	Questback does not use personal data from respondents for automated decision making. If Questback's customers do so, they will describe it when setting up a survey, and the respondents will be informed accordingly before any consent is provided
Formal	Does Questback have any documents or policies documenting its work towards compliance with the GDPR?	Yes. Questback has all policies documented as part of its Binding Corporate Rules.
	Do you have an appointed Data Protection Officer?	Yes: Arve Føyen, Lawyer/Partner Mobile: +47 91 81 99 62 Address: Advokatfirmaet Føyen Torkildsen AS C.J. Hambros plass 2 D, 0164 Oslo, P.O. Box 7086 St. Olavs plass, NO-0130 Oslo Norway Swbd: +47 21 93 10 00, E-mail: af@foyentorkildsen.no www.foyentorkildsen.no
	What is Questback's procedure in case of complaints?	Respondents who wish to raise complaints must refer to the controller, Questback's customers. Respondents will be informed, and directed to the controller in question. Any complaints to Questback as controller can be raised to data protection officers, whose contact information is listed on our webpage
	Does Questback have a Data Protection Officer?	Yes
EMPLOYEES	Does Questback have confidentiality clauses in place with all employees?	Yes
	Do the terms and conditions of employment for Questback employees clearly state the requirement to follow information security policy and procedures?	Yes

Questback HQ
Bogstadveien 54
0366 Oslo
NORWAY

TOPIC	QUESTION	Questback answer
	What referencing, security and ID checks are performed on personnel?	Due to variation in local legislation, staff forms vary between Questback entities.
	Is information security and data protection training undertaken by all personnel prior to being given access to personal data?	All Questback personnel are provided with training, information and materials on a general level, and specifically for their role when required.
	Does Questback have a disciplinary process in place to take action against personnel who have committed a security breach?	All Questback personnel have a clear commitment to company policies on privacy and security in their employment agreement, and breach would therefore follow standard disciplinary procedures
Data Collection	How does Questback allow its customers to obtain and document expressed permission to store people's personal data?	Consent from respondents will be collected as part of the survey, assisted by functionality in the software that by default will lead the user to build surveys with information required to collect valid consent. Respondents will be provided with all information required to provide valid consent under GDPR, hereunder purpose defined by customer, and retention time defined by customer.
Physical and Technical measures	What technical provisions are in place to defend against cyber-attacks?	Our data center is ISO 27001 BSI certified. We are using Watchguard firewalls with IDS to defend against attacks.
	Are industry-standard encryption algorithms and technologies employed for transferring, storing, and receiving individuals' sensitive personal information?	Essentials is accessed via https only. Certificate vendor is COMODO. Our data center is ISO 27001 BSI certified.
	What are backup and restore procedures in relation to Customer personal data in the event of data loss?	Essentials is backed up daily to disk and tape. Disk is overwritten after 10 days, tapes are overwritten after 8 weeks.
	Do your systems undergo regular penetration testing?	Yes, at least yearly
	What are Questback's access control policies for both customer and internal data?	Internal access to data is limited to IT-OPS member for Essentials. Customers do not have access to internal data. Customers have a access to their data via https.
	Where is Customer' personal data physically stored?	User and respondent data is stored with the software in secure data halls in Frankfurt, Germany.

Questback HQ
Bogstadveien 54
0366 Oslo
NORWAY

TOPIC	QUESTION	Questback answer
	Who has access to Questback's data facilities?	Data in Questback software is accessed by the following: Customer's users Questback support personnel, for the purpose of providing support If relevant under contract with customer, Questback consultants
Privacy Management	What are the terms of ownership over data processed by Questback?	Personal data is owned solely by the data subject, as dictated by applicable privacy law, and the new General data Protection Regulations. Ownership to data entered into Questback's system by customer, or by customers' respondents, is not transferred to Questback
	Is Questback's data security team able to discover and identify personal data, even when not stored together with other identifiers?	Questback is able to identify typical personal data (names, IP address, e-mail address etc). However, as the definition of personal data covers a very wide area, and Questback's customers are free to collect any type of data in free text or otherwise, Questback cannot itself have a complete overview. Questback has therefore created functionality, available in spring release 2018, that will give its customers full rights to define where personal data will or may be collected.
	How does Questback handle instances when customers or prospects request their data be removed from your system(s)?	Users will have access to remove their data from the systems themselves. Respondents will be requested to contact customer, who is the controller. When customer has identified the Respondent, and request Questback to delete data for this particular respondent in its systems, Questback will perform the task manually. Functionality that will allow customer to perform the task itself will be available in later release.
	What third party organizations does Questback work with that may also have access to the personal data processed on behalf of customers?	A list of subprocessors is provided in annex to the Attached Data Processing Agreement.
Data Breach Readiness	Does Questback have a documented privacy and security Incident Response Plan?	Yes, such plan is defined on high level in Questback Binding Corporate Rules. Detailed plans are being developed and will be in place before May 25th
	What is Questback's formal procedure for reporting out on data breaches / leaks?	Detailed plans are being developed and will be in place before May 25th

Questback HQ
Bogstadveien 54
0366 Oslo
NORWAY

TOPIC	QUESTION	Questback answer
	Does Questback operate an Information Security Management System?	Yes.
	Is Questback certified to such standard as ISO27001?	Storage facilities are certified under ISO27001
	How often does Questback execute vulnerability scans?	At least yearly
	Can Questback share the results from its most recent vulnerability scan?	As vulnerability scans may include sensitive elements, we cannot freely share the tests. Summary of penetration test may be provided subject to NDA.