

Data Protection Policy & Procedure

Contents

1. Purpose	2
2. Scope	2
3. Policy Statement	2
3.1 Privacy by Design	2
3.2 Compliance Monitoring	2
3.3 Data Protection Principles	3
3.4 Data Collection	3
3.5 Data Processing	4
3.6 Data Quality	5
3.7 Digital Marketing	5
3.8 Data Retention	6
3.9 Data Protection	6
3.10 Data Subject Requests	6
3.11 Law Enforcement Requests & Disclosures	7
3.12 Data Protection Training	7
3.13 Data Transfers	7
3.14 Complaints Handling	7
3.15 Breach Reporting	8
3.16 Support, Advice and Communication	8
4. Roles & Responsibilities	8
5. Definitions	8
6. Document Management	9

1. Purpose

This policy establishes an effective, accountable and transparent framework for ensuring compliance with the requirements of the GDPR (General Data Protection Regulation).

2. Scope

This policy applies to all BCQ Group employees and all third parties responsible for any sub-processing of personal data on behalf of BCQ Group and its customers.

3. Policy Statement

BCQ Group is committed to conducting its business in accordance with all applicable data protection laws and regulations and in line with the highest standards of ethical conduct.

This policy sets forth the expected behaviours of BCQ Group's employees and third parties in relation to the collection, use, retention, transfer, disclosure and destruction of any personal data belonging to a BCQ Group contact (i.e. the data subject).

Personal data is any information (including opinions and intentions) that relates to an identified or identifiable natural person. Personal or Special Category data is subject to certain legal safeguards and other regulations that impose restrictions on how organisations may process Personal or Special Category data. An organisation that processes Personal or Special Category data and makes decisions about its use is known as a Data Controller and BCQ Group is a Data Controller in terms of its employees. An organisation that follows instructions from someone else regarding the processing of the data is a Data Processor - BCQ Group is a Data Processor for its customers.

BCQ Group is responsible for ensuring compliance with the data protection requirements as both Data Controller & Processor outlined in this policy. Non-compliance may expose BCQ Group to complaints, regulatory action, fines and/or reputational damage.

BCQ Group's leadership is fully committed to ensuring continued and effective implementation of this policy and expects all BCQ Group employees and third parties to share in this commitment. Any breach of this policy will be taken seriously and may result in disciplinary action or business sanction.

3.1 Privacy by Design

To ensure that all data protection requirements are identified and addressed when designing new systems or processes and/or when reviewing or expanding existing systems or processes, each of them must go through an approval process before continuing. Each BCQ Group business area must ensure that a Data Protection Impact Assessment (DPIA) is conducted, in cooperation with the Strategic Performance Director, for all new and/or revised systems or processes for which it has responsibility.

The subsequent findings of the DPIA must then be submitted to the Operations & Technical Director for review and approval. Where applicable, the Information Technology Infrastructure Group, as part of its IT strategies and application design review process, will cooperate with the Strategic Performance Director to assess the impact of any new technology uses on the security of Personal and Special Category data.

3.2 Compliance Monitoring

To confirm that an adequate level of compliance that is being achieved by all BCQ Group business areas in relation to this policy, the Operations & Technical Director will carry out an annual data protection compliance audit for all such business areas and processes. Each audit will, as a minimum, assess:

• **Compliance with policy in relation to the protection of personal & sensitive data, including:**

- ✓ The assignment of responsibilities.
- ✓ Raising awareness.
- ✓ Training of employees.

• **The effectiveness of data protection-related operational practices, including:**

- ✓ Data subject rights.
- ✓ Personal data transfers.
- ✓ Personal data incident management.
- ✓ Personal data complaints handling.
- ✓ The level of understanding of data protection policies and privacy notices.
- ✓ The currency of data protection policies and privacy notices.
- ✓ The accuracy of personal data being stored.
- ✓ The conformity of data processor activities.
- ✓ The adequacy of procedures for redressing poor compliance and personal data breaches. The Strategic Performance Director, in cooperation with key business stakeholders from each BCQ Group business area, will devise a plan with a schedule for correcting any identified deficiencies within a defined and reasonable time frame. Any major deficiencies and good practice identified will be reported to, monitored and shared by the BCQ Group Executive Team.

3.3 Data Protection Principles

BCQ Group has adopted the following GDPR Principles to govern its collection, use, retention, transfer, disclosure and destruction of personal data:

Principle 1: Lawfulness, Fairness and Transparency. Personal and Special Category data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject. This means that BCQ Group must tell the data subject (where BCQ are the Data Controller) what processing will occur (transparency), the processing must match the description given by the Customer (fairness), and it must be for one of the purposes specified in the applicable data protection regulation (lawfulness).

Data Protection Policy Effective Date: 12/04/2018

Principle 2: Purpose Limitation. Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. This means BCQ Group must (where BCQ are the Data Controller) specify exactly what the personal data collected will be used for and limit the processing of that personal data to only what is necessary to meet the specified purpose.

Principle 3: Data Minimisation. Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. This means BCQ Group must not store any personal data beyond what is strictly required.

Principle 4: Accuracy. Personal data shall be accurate and kept up to date. This means BCQ Group must have processes in place for identifying and addressing out-of-date, incorrect and redundant personal data.

Principle 5: Storage Limitation. Personal data shall be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed. This means BCQ Group must, wherever possible, store personal data in a way that limits or prevents identification of the data subject.

Principle 6: Integrity & Confidentiality. Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing, and against accidental loss, destruction or damage. BCQ Group must use appropriate technical and organisational measures to ensure the integrity and confidentiality of personal data is maintained at all times.

Principle 7: Accountability. The Data Controller shall be responsible for and be able to demonstrate compliance. This means BCQ Group must demonstrate that the six data protection principles (outlined above) are met for all personal data for which it is responsible.

3.4 Data Collection

Data Sources

Personal data should be collected only from the data subject unless one of the following apply:

- The nature of the business purpose necessitates collection of the personal data from other persons or bodies.
- The collection must be carried out under emergency circumstances in order to protect the vital interests of the data subject or to prevent serious loss or injury to another person.

If personal data is collected from someone other than the data subject, the data subject must be informed of the collection unless one of the following apply:

- The data subject has received the required information by other means.
- The information must remain confidential owing to a professional secrecy obligation.
- A national law expressly provides for the collection, processing or transfer of the personal data.

Where it has been determined that notification to a data subject is required, notification should occur promptly, but in no case later than:

- One calendar month from the first collection or recording of the personal data.
- At the time of first communication if used for communication with the data subject.
- At the time of disclosure if disclosed to another recipient.

Data Subject Consent

BCQ Group will obtain personal data only by lawful and fair means and, where appropriate with the knowledge and consent of the individual concerned. Where a need exists to request and receive the consent of an individual prior to the collection, use or disclosure of their personal data, BCQ Group is committed to seeking such consent.

Data Subject Notification

BCQ Group will, when required by applicable law, contract, or where it considers that it is reasonably appropriate to do so, provide data subjects with information as to the purpose of the processing of their personal data. When the data subject is asked to give consent to the processing of personal data and when any personal data is collected from the data subject, all appropriate disclosures will be made, in a manner that draws attention to them, unless one of the following apply:

- The data subject already has the information;
- A legal exemption applies to the requirements for disclosure and/or consent. The disclosures may be given orally, electronically or in writing. If given orally, the person making the disclosures should record via email or other written form which then should be retained, along with a record of the facts, date, content, and method of disclosure.

External Privacy Notices

Each external website provided by BCQ Group will include an online 'Privacy Notice' and an online 'Cookie Notice' fulfilling the requirements of applicable law.

3.5 Data Processing

BCQ Group uses the personal data of its contacts for the following broad purposes:

- The general running and business administration of BCQ Group services.
- To provide services to BCQ Group's customers and stakeholders.
- The ongoing administration and management of customer services.

The use of a contact's information should always be considered from their perspective and whether the use will be within their expectations or if they are likely to object. For example, it would clearly be within a contact's

expectations that their details will be used by BCQ Group to respond to a contact request for information about the products and services on offer. However, it will not be within their reasonable expectations that BCQ Group would then provide their details to third parties for marketing purposes.

BCQ Group will process personal data in accordance with all applicable laws and applicable contractual obligations. More specifically, BCQ Group will not process personal data unless at least one of the following requirements are met:

- The data subject has given consent to the processing of their personal data for one or more specific purposes.
- Processing is necessary for the performance of a contract to which the data subject is party or, in order to take steps at the request of the data subject prior to entering into a contract.
- Processing is necessary for compliance with a legal obligation to which the Data Controller is subject.
- Processing is necessary in order to protect the vital interests of the data subject or of another natural person.
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Data Controller.
- Processing is necessary for the purposes of the legitimate interests pursued by the Data Controller or by a third party (except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject, in particular where the data subject is a child).

There are some circumstances in which personal data may be further processed for purposes that go beyond the original purpose for which the personal data was collected. When making a determination as to the compatibility of the new reason for processing, guidance and approval must be obtained from the Operations & Technical Director/Strategic Performance Director before any such processing may commence.

3.6 Data Quality

Where BCQ Group are the Data Controller, the organisation will adopt all necessary measures to ensure that the personal data it collects is complete and accurate in the first instance and is updated to reflect the current situation of the data subject. The measures adopted by BCQ Group to ensure data quality include:

- Correcting personal data known to be incorrect, inaccurate, incomplete, ambiguous, misleading or outdated, even if the data subject does not request rectification.
- Keeping personal data only for the period necessary to satisfy the permitted uses or applicable statutory retention period.
- The removal of personal data if in violation of any of the data protection principles or if the personal data is no longer required.
- Restriction, rather than deletion of personal data, insofar as:
 - ✓ a law prohibits erasure
 - ✓ erasure would impair legitimate interests of the data subject.
 - ✓ the data subject disputes that their personal data is correct, and it cannot be clearly ascertained whether their information is correct or incorrect.
- In any circumstance where consent has not been gained for the specific processing in question, BCQ Group will address the following additional conditions to determine the fairness and transparency of any processing beyond the original purpose for which the personal data was collected: any link between the purpose for which the personal data was collected and the reasons for intended further processing.
- The context in which the personal data has been collected, particularly regarding the relationship between data subject and the Data Controller.
- The nature of the personal data, particularly whether special categories of data are being processed, or whether personal data related to criminal convictions and offences are being processed.

- The possible consequences of the intended further processing for the data subject.
- The existence of appropriate safeguards pertaining to further processing, which may include encryption, anonymisation or pseudonymisation.

Where BCQ Group are the Data Processor, on behalf of their customer, the organisation will only carry out any processing as specifically requested in writing by the customer relating to the job.

3.7 Digital Marketing

As a general rule, BCQ Group will not send promotional or direct marketing material to a BCQ Group contact through digital channels such as mobile phones, email and the Internet, without first obtaining their consent. Any BCQ Group business area wishing to carry out a digital marketing campaign without obtaining prior consent from the data subject must first have it approved by a Director.

Where personal data processing is approved for digital marketing purposes, the data subject must be informed at the point of first contact that they have the right to object, at any stage, to having their data processed for such purposes. If the data subject puts forward an objection, digital marketing related processing of their personal data must cease immediately, and their details should be kept on a suppression list with a record of their opt-out decision, rather than being completely deleted.

It should be noted that where digital marketing is carried out in a 'business to business' context, there is no legal requirement to obtain an indication of consent to carry out digital marketing to individuals provided that they are given the opportunity to opt-out.

3.8 Data Retention

To ensure fair processing, personal data will not be retained by BCQ Group for longer than necessary in relation to the purposes for which it was originally collected, or for which it was further processed. The length of time for which BCQ Group need to retain personal data is set out in BCQ Group's 'Data Retention Policy'.

This takes into account the legal and contractual requirements, both minimum and maximum, that influence the retention periods set forth in the schedule. All personal data should be deleted or destroyed as soon as possible where it has been confirmed that there is no longer a need to retain it.

Where data is held for processing by BCQ Group on behalf of its customers and stakeholders, the retention period will be subject to the individual job and customer contract terms but where no such terms have been set out, BCQ will ensure all processing data is deleted from all servers no longer than 90 days.

3.9 Data Protection

BCQ Group will adopt physical, technical, and organisational measures to ensure the security of personal data. This includes the prevention of loss or damage, unauthorised alteration, access or processing, and other risks to which it may be exposed by virtue of human action or the physical or natural environment. A summary of personal data-related security measures is provided below:

- Prevent unauthorised persons from gaining access to data processing systems in which personal data is processed.
- Prevent persons entitled to use a data processing system from accessing personal data beyond their needs and authorisations.
- Ensure that personal data in the course of electronic transmission during transport cannot be read, copied, modified or removed without authorisation.
- Ensure that access logs are in place to establish whether, and by whom, the personal data was entered into, modified on or removed from a data processing system.
- Ensure that in the case where processing is carried out by BCQ Group, the data can be processed only in accordance with the instructions of the Data Controller.
- Ensure that personal data is protected against undesired destruction or loss.
- Ensure that personal data collected for different purposes can and is processed separately.

- Ensure that personal data is not kept longer than necessary.

3.10 Data Subject Requests

The Operations & Technical Director will establish a system to enable and facilitate the exercise of data subject rights related to:

- Information access.
- Objection to processing.
- Objection to automated decision-making and profiling.
- Restriction of processing.
- Data portability.
- Data rectification.
- Data erasure.

If an individual makes a request relating to any of the rights listed above, BCQ Group will consider each such request in accordance with all applicable data protection laws and regulations. No administration fee will be charged for considering and/or complying with such a request unless the request is deemed to be unnecessary or excessive in nature. Data subjects are entitled to obtain, based upon a request made in writing to the Operations & Technical Director or email to: DPO@bcqgroup.com.

It should be noted that situations may arise where providing the information requested by a data subject would disclose personal data about another individual. In such cases, information must be redacted or withheld as may be necessary or appropriate to protect that person's rights. Detailed guidance for dealing with requests from data subjects can be found in BCQ Group's 'Data Subject Access Rights Policy and Procedure' document.

3.11 Law Enforcement Requests & Disclosures

In certain circumstances, it is permitted that personal data be shared without the knowledge or consent of a data subject. This is the case where the disclosure of the personal data is necessary for any of the following purposes:

- The prevention or detection of crime.
- The apprehension or prosecution of offenders.
- The assessment or collection of a tax or duty.
- By the order of a court or by any rule of law.

If BCQ Group processes personal data for one of these purposes, then it may apply an exception to the processing rules outlined in this policy but only to the extent that not doing so would be likely to prejudice the case in question. If any BCQ Group employee receives a request from a court or any regulatory or law enforcement authority for information relating to a BCQ Group employee or customer/stakeholder, you must immediately notify the Operations & Technical Director or any other Director who will provide comprehensive guidance and assistance.

3.12 Data Protection Training

All BCQ Group employees that have access to personal data will have their responsibilities under this policy outlined to them as part of their staff induction training. In addition, BCQ Group Operations & Technical Director/ Strategic Performance Director will provide regular Data Protection training and procedural guidance for all staff and at a level pertinent to their roles and responsibilities.

3.13 Data Transfers

BCQ Group, as Data Processor on behalf of their customers/stakeholders may transfer personal data to internal or third-party recipients located in the UK. No data will be processed or transferred to a third party outside of the UK. BCQ Group may only transfer personal data where one of the transfer scenarios listed below applies:

- The data subject/customer/stakeholder has confirmed proper consent to the proposed transfer.
- The transfer is necessary for the performance of a contract with the data subject / customer / stakeholder.
- The transfer is necessary for the implementation of pre-contractual measures taken in response to the data subject / customer / stakeholder's request.
- The transfer is necessary for the conclusion or performance of a contract concluded with a third party in the interest of the data subject / customer / stakeholder.
- The transfer is legally required on important public interest grounds.
- The transfer is necessary for the establishment, exercise or defence of legal claims.
- The transfer is necessary in order to protect the vital interests of the data subject

3.14 Complaints Handling

Data subjects with a complaint about the processing of their personal data, should put forward the matter in writing to DPO@bcqgroup.com. An investigation of the complaint will be carried out to the extent that is appropriate based on the merits of the specific case. The Operations & Technical Director and/or another Director in their absence will inform the data subject of the progress and the outcome of the complaint within a reasonable period. If the issue cannot be resolved through consultation between the data subject and the Operations & Technical Director then the data subject may, at their option, seek redress through mediation, binding arbitration, litigation, or via complaint to the Data Protection Authority within the applicable jurisdiction via <https://ico.org.uk/make-a-complaint/your-personal-information-concerns>

3.15 Breach Reporting

Any individual who suspects that a personal data breach has occurred as a result of the theft, exposure, unintended access, processing without consent of personal data must immediately notify the Operations & Technical Director providing a description of what occurred. Notification of the incident can be made via email DPO@bcqgroup.com, by calling, or by using the independent Whistleblowing Advice Line: 020 7404 6609.

The Operations & Technical Director will investigate all reported incidents to confirm whether or not a personal data breach has occurred. If a personal data breach is confirmed, Operations & Technical Director will follow the relevant authorised procedure based on the criticality and quantity of the personal data involved, following and complying with UK Data Protection Regulations and timescales. For severe personal data breaches, the BCQ Group Executive Board Team will initiate and chair an emergency response team to coordinate and manage the personal data breach response.

All incidents of data breach and/or potential data breach incidents (either as a Controller or Processor of the data) will be recorded, investigated and any preventative actions addressed by the Operations & Technical Director/ Strategic Performance Director.

3.16 Support, Advice and Communication

For advice and support in relation to this policy and procedure, please contact the BCQ Group Strategic Performance Director on 01280 824000.

4. Roles & responsibilities

BCQ Group Executive Board are ultimately responsible for Data Protection, its processing and compliance within the Group.

Employees responsible for the processing of personal data are aware of and comply with the contents of this policy.

In addition, each BCQ Group business area will ensure all third parties engaged to process personal data on their behalf (i.e. benefit providers) are aware of and comply with the contents of this policy. Assurance of such

compliance must be obtained from all third parties, whether companies or individuals, prior to granting them access to personal data controlled by BCQ Group.

5. Related Documents

BCQ Group's Privacy Policy

ISO27001 IT Security Standard

Non-Disclosure Agreement

Employment Contract – Confidentiality Agreement

Sub-Processor Data Protection Agreement

Legal Register

Data Retention Policy – current in draft awaiting approval

Camera Policy – currently in draft awaiting approval

'Data Subject Access Rights Policy and Procedure' document – currently in draft awaiting approval

6. Document Management

Prepared By:	Mark Wiseman Operations & Technical Director	Date & Signature	<i>M Wiseman</i> 13/02/2020
Approved By:	Mark Wiseman Operations & Technical Director	Date & Signature	<i>M Wiseman</i> 13/02/2020

Change Record

Issue & Date Ref:	Author of Change	Section(s) Affected	Description of Change / Request for Change
Issue 1.	Anita Wise	ALL	Release of Procedure
Issue 2.	Mark Wiseman	ALL	Change of branding and replacement of HR & Operations Director and Compliance Manager