BGC HOLDINGS LTD
DATA PROTECTION POLICY

Introduction
This document sets out the data protection arrangements we have established for BGC Holdings Ltd, and all subsidiaries and associated companies (hereinafter referred to as the 'Company').

The need to retain and protect personal data varies widely with the type of data held by the Company. Some personal data can be immediately deleted while other data will need to be retained into the future. This policy seeks to describe the company's policy for specific data retention, protection and deletion.

The scope of this policy covers all company data stored on company-owned, company-leased, and otherwise company-provided systems and media.

Regulation
The Company is required to comply with the General Data Protection Regulation 2016 (GDPR), the Data Protection Act 1998 and the Data Protection (Amendment) Act 2003. In August 2017, the Government passed the Data Protection Bill which will bring the GDPR into UK law. There are some instances, however, where other legislation and regulations will supersede the GDPR and these are detailed below.

In the event of a data loss, destruction or transmission, The Company will be obliged to report this to the individual or company affected, as well as the Information Commissioner's Office (ICO) which has power to impose a financial penalty for a breach up to €20 million or 4% of worldwide turnover. There is a mandatory requirement to report the breach to the individual and to the ICO within 72 hours of The Company becoming aware of it.

The ICO has advised that all UK businesses will need to comply with GDPR despite Brexit. This is because it will affect all data subjects in Europe or carrying out processing of data in Europe or about European data subjects.

Personal Data
The Company collects personal data such as name, address, phone number, email address, and bank details which are used by us in the course of employment for legitimate interests under GDPR. We only collect the personal data that we need, and we shall ask employees for their formal permission to do so when they commence employment with us.

Employment by The Company
To comply with our contractual, statutory, and management obligations and responsibilities, we process personal data, including 'sensitive' personal data, from job applicants and our employees. Such data includes information relating to health, employment history and any criminal convictions. In certain circumstances, we may process personal data or sensitive personal data, without explicit consent. Further information on what data is collected and why it's processed is given below.

Contractual responsibilities include those arising from the contract of employment. The data processed to meet contractual responsibilities includes data relating to payroll, bank account, postal address, sick pay, annual leave, maternity/paternity pay, pensions and emergency contacts.

Statutory responsibilities are imposed through law on the company as an employer. The data processed to meet our statutory responsibilities includes data relating to tax, national insurance, statutory sick pay, statutory maternity/ paternity pay, family leave, work permits, equal opportunities monitoring.

Management responsibilities are related to the functioning of the company. The data processed to meet management responsibilities includes data relating to recruitment and employment, training and development, absence for whatever reasons, disciplinary matters, email address and telephone number.

Sensitive Personal Data
GDPR defines 'sensitive personal data' as information about racial or ethnic origin, political opinions, religious beliefs or other similar beliefs, trade union membership, physical or mental health, sexual life, and criminal allegations, proceedings or convictions.

In certain limited circumstances, we may legally collect and process sensitive personal data without requiring the explicit consent of an employee.

(a) We will process data about an employee's health where it is necessary, for example, to record absence from work due to sickness, to pay statutory sick pay, to make appropriate referrals to our Occupational Health Provider, and to make any necessary arrangements or adjustments to the workplace in the case of disability. This processing will not normally happen without the employee's knowledge and, where necessary, consent.

(b) We will process data about, but not limited to, an employee's racial and ethnic origin, their sexual orientation or their religious beliefs only where they have volunteered such data and only for the purpose of monitoring and upholding our equal opportunities policies and related provisions.

(c) Data about an employee's criminal convictions will be held as necessary.

Sharing Data with Third Parties
In order to carry out our contractual and management responsibilities, we may, from time to time, need to share an employee's personal data with one or more third party supplier.

To meet the employment contract, we are required to transfer an employee's personal data to third parties, for example, to pension providers and HM Revenue & Customs. To fulfil our statutory responsibilities, we're required to give some of an employee's personal data to government departments or agencies e.g. provision of salary and tax data to HM Revenue & Customs.

Data Retention
It is not practical or cost-effective to save all data. Some data must be retained to protect The Company's interests, preserve evidence and audit trails, while generally conforming to good business practices. Reasons for data retention include:

- Litigation.
- Accident Investigation.
- Regulatory requirements.
- HMRC requirements.
- Intellectual property preservation.

As data storage increases in size and decreases in costs, companies often err on the side of storing data in several places on the IT network. A common example of this is where a single file may be stored on a local user's machine, on a central file server, and on back-up system.

When identifying and classifying the Company's data it is important to understand where that data is stored, particularly for duplicate copies, so that this policy may be applied to all duplicates of the information.

Data Retention Requirements
This section sets out the agreed guidelines for retaining the different types of company data that are held by The Company:

- Customer data will be held for as long as the organisation remains a customer of the Company, plus 6 years.

- Personal employee data will be held for the duration of employment and then for 6 years after the last date of contractual employment.
- Employee contracts will be held for 3 years after the last day of contractual employment.
- Company and employee tax related payment records will be held for 6 years.
- VAT records will be held for 6 years.
- Recruitment details including interview notes and CVs will be held for 1 year after the interview. This personal data will then be destroyed.
- Health & Safety records will be retained indefinitely.

If any data retained under this policy is stored in a secure network folder accessible by restricted personnel only. Reference to the Managing Director should be made if there is any doubt as to how data is stored.

Data Destruction
Data destruction is a critical part of the data retention policy. Data destruction ensures that the Company uses data efficiently thereby making data management and data retrieval more cost effective. There are good reasons to delete data after a reasonable amount of time. These include the following:

- It is easier to keep more limited amounts of data secure.
- It is easier to find specific data in a response to a Subject Access Request, or when searching data for other purposes.
- It is consistent under GDPR to securely delete data that is no longer required for its original purpose.
- If it is retained for a long period, it is more likely to be inaccurate and out of date.

When the above timeframe expires, company staff must actively destroy the data covered by this policy. If a user feels that certain data should not be destroyed, they should identify the data to their line manager so that an exception to the policy can be considered. Exceptions may only be approved by the Managing Director of the Company.

At present there is no automated facility by which emails, and files can be automatically destroyed. It will be necessary to carry out these tasks manually. Consideration should be given to mapping data flows in a Data Privacy Impact Assessment (DPIA) to identify the different locations and format of data held.

If security is not maintained and there is a data loss, the fact that excessive data has been retained, and therefore put at risk, is a factor which the ICO will take into account when considering whether to impose a civil penalty and the level of that penalty. The breach is more likely to be regarded as serious if no old data has ever been deleted, if there is no data retention policy, or if no thought has been given to whether old data should be deleted.

The Company specifically directs users not to destroy data in violation of this policy. Destroying data that a user may feel is harmful to themselves is expressly forbidden, as is destroying data in an attempt to cover up a violation of law or company policy.

Enforcement

This policy will be enforced by the Managing Director of The Company. Violations will result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities or theft of company property (physical or intellectual) are suspected, the company may report such activities to the applicable authorities.

Subject Access Requests
If you would like further information on your rights or wish to exercise them, please contact the Managing Director. You will be asked to provide the following details:

- The personal information you want to access.
- Where it is likely to be held.
- The date range of the information you wish to access.

We will also need you to provide information that will help us confirm your identity. If we hold personal information about you, we will give you a copy of the information in an understandable format together with an explanation of why we hold and use it. Once we have all the information necessary to respond to your request we'll provide your information to you within one month. This timeframe may be extended by up to two months if your request is particularly complex.

Data Breach Process
If you become aware of a breach of the Data Protection Act, the GDPR or its obligations under a client contract, you must inform the Managing Director immediately who will report the incident immediately to our client and the ICO. A Data Breach Report must be completed and passed to the Managing Director.

A data breach will include, but not be limited to:

- Any loss, destruction or inappropriate transmission of personal data.
- This will relate to both client and Company employees.

The Managing Director is responsible for any investigation, escalation and resolution measures deemed necessary as the result of an incident and will maintain a log of all security incidents.

When a security incident is reported, a decision will have to be made to whether an investigation into the incident will be carried out and who will be tasked to carry out the investigation.

Where a follow-up action against a person or organisation after an information security incident involves legal action (either civil or criminal) evidence should be collected, retained, and presented to conform to the rules for evidence laid down in the relevant jurisdiction(s).

The Managing Director will advise on the appropriate course of action and any further actions to be taken. Security investigations must address the following:

- What happened and its impact?
- Root cause analysis of why it happened and how?
- What needs to be done immediately to prevent further damage and facilitate initial recovery?
- What needs to be done in the longer term to prevent a further occurrence?
- Identify if any person is culpable and whether disciplinary action is necessary.

For all investigations, a record must be maintained throughout the conduct of the investigation and the resolution of the breach. Investigation records must include:

- Nature of the breach.
- When, how and who discovered the breach?
- To whom and when was the breach escalated?
- Details of actions taken, when, and by whom, together with results.
- Details of any emergency measures implemented to contain the exposure.
- Details of agreed permanent solution.
- Impact assessment.

A decision on the need to inform the client and the ICO will be taken by the Managing Director. Under GDPR, both the client and the ICO must be informed of any personal data breach within 72 hours of the Company becoming aware of it.

Changes to this Data Protection Policy
The Directors may amend this policy to ensure it remains up to date and reflects how and why we use your personal data and new legal requirements. You will be advised of any future changes and asked to confirm your understanding and acceptance.