C&A Data Protection Policy

Introduction

As a Firm Cooke & Arkwright from time to time need to gather and hold certain information about individuals for business purposes.

These can include employees, clients, suppliers, business contacts and other people the organisation has a relationship with or may need to contact.

This policy describes how this personal data must be collected, handled and stored to meet the company's data protection standards and to comply with the law.

We adhere with the requirements of the General Data Protection Regulation (GDPR) which replaces the Data Protection Act 1998.

This policy sets out how we seek to protect personal data and ensure that all staff understand the rules governing their use of personal data to which they have access in the course of their work.

Our Data Protection Policy exists to ensure that Cooke & Arkwright:

- Complies with GDPR law and follow good practice within the firm
- Protects the rights of staff, clients and other interested parties
- Is open about how it stores and processes individuals' data
- Protects itself from the risks of a data breach

As a Firm we define a client, supplier, business contact, employee and any other person the organisation has a relationship with, where we hold personal data as a "Data subject".

A data subject is a person that can be identified, directly or indirectly, in particular by reference to an identification number (i.e. Passport number, telephone, DOB, House address etc.) or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.

We define Personal data as:

Information relating to identifiable individuals, such as job applicants, current and former employees, agency, contract and other staff, clients, suppliers and marketing contacts.

Personal data we gather may include: individuals' contact details, educational background, financial and pay details, details of certificates and diplomas, education and skills, marital status, nationality, job title, and CV.

We may need to retain personal data but will do so for no longer than is necessary. What is necessary will depend on the circumstances we obtained the information for "Business Purposes", taking into account the reasons that the personal data was obtained.

For the purpose of GDPR we define the use of personal data for "Business Purposes" as:

Personnel, administrative, financial, regulatory, payroll and business development purposes.

- Compliance with our legal, regulatory and corporate governance obligations and good practice
- Gathering information as part of investigations by regulatory bodies or in connection with legal proceedings or requests
- Ensuring business policies are adhered to (such as policies covering email and internet use)
- Operational reasons, such as recording transactions, training and quality control, ensuring the confidentiality of commercially sensitive information, security vetting, credit scoring and checking
- Investigating complaints
- Monitoring staff conduct, disciplinary matters
- Marketing our business
- Engaging with customers in the areas of sales and lettings.

We will only hold Data for the period necessary for the purpose and also to comply with Legal or Regulatory Requirements.

Data Accuracy and relevance

We ensure that any personal data we process is accurate, adequate, relevant and not excessive, given the purpose for which it was obtained. We will not process personal data that is not for a business related purpose, unless the individual concerned has agreed to this or would otherwise reasonably expect this.

We will always abide by any request from an individual not to use their personal data for direct marketing purposes and notify the relevant data handler in the Firm about any such request.

Individuals may ask that we correct inaccurate personal data relating to them. If a member of staff believes that information on a client or external party is inaccurate they should record the fact that the accuracy of the information is disputed and inform a Director of the Firm. If the data subject contacts a member of staff at Cooke & Arkwright, you must ensure you respond to this request and reply in writing to the data subject, that you have processed their request.

We do not send direct marketing material to someone electronically (e.g. via email) unless we have an existing business relationship with them in relation to the services being marketed or we have had consent.

Any data subject has the right to be forgotten. If we receive a request that information held on a data subject is requested to be deleted or removed, we will honour all requests, unless there is a explicit extenuating circumstances that the Firm can justify for the need to be retained.

Data Protection Training:

All staff receive training on our GDPR policy. Further training is then provided on an bi annual basis, which is compulsory or whenever there is a substantial change in the law or our policy and procedure.

Training is provided through an in-house seminar.

It will cover:

- The law relating to data protection
- Our data protection and related policies and procedures.

Data Protection Principles

As a Firm we will always adhere to the 6 GDPR Principles:

1. **Lawfulness, fairness and transparency**
Personal data shall be processed fairly and lawfully.
We will always ensure transparency and tell a data subject what data processing will be done. We endeavour that how we process and handle data is reflected in our policies, procedures and as described in any documentation.

All information we hold will be stored and processed as per specified in the GDPR.

We will ensure that:
We have legitimate grounds for collecting and using the personal data;
Not use the data in ways that have unjustified adverse effects on the individuals concerned;
Be transparent about how we intend to use the data, and give individuals appropriate privacy notices when collecting their personal data;
Handle people's personal data only in ways they would reasonably expect; and
make sure we do not do anything unlawful with the data.

2. **Purpose limitations**
Personal data will only be obtained for "specified, explicit and legitimate purposes". Data will only be used for a specific processing purpose that the subject has been made aware of and no other, without further consent.

We strive to ensure that the Firm is open about their reasons for obtaining personal data, and that what we do with the information is in line with the reasonable expectations of the individuals concerned.

3. **Data minimisation**
We will only collect data on a subject that is "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed". We do not expect to need further data in our normal business activity, unless explicitly explained to the data subject.

4. **Accuracy**
We always ensure that the data we hold on a subject is "accurate and where necessary kept up to date"

As a firm we will always take reasonable steps to ensure the accuracy of any personal data we obtain. Alongside this we will check that the source of any personal data is clear and accurate and the source(s) are from the Data Subject themselves.

5. **Storage limitations**
We will not retain personal data longer than is necessary for the purpose it was obtained. We ensure that we dispose of data when it is no longer needed, to reduce the risk that it will become inaccurate, out of date or irrelevant, this can vary depending on reason for holding the data and on going business relationships.

6. **Integrity and confidentiality**
As a Business we ensure that all members of staff that process or handle data undertake all procedures correctly and are aware of the importance of confidentiality and deal with any data "in a manner [ensuring] appropriate security of the personal data including protection against unlawful processing or accidental loss, destruction or damage".
We are willing and able to provide the following to a data subject:

- The right of access to a copy of the information comprised for a data subject;
- Their right to object to processing that is likely to cause or is causing damage or distress;
- A right to prevent processing for direct marketing;
- A right to object to decisions being taken by automated means;
- A right in certain circumstances to have inaccurate personal data rectified, blocked, erased or destroyed

Privacy Policy

The Firm also has a Privacy Policy available on the Corporate website, or upon request.

The privacy policy sets out the following:

- The purposes for which we hold personal data on clients, suppliers, business contacts, employees and other people the organisation has a relationship with or may need to contact, which is dependant on the business purpose.
- Highlights that our work may require us to give information to third parties such as expert witnesses and other professional advisers
- Provides that customers have a right of access to the personal data that we hold about them
- States we do not sell or share data without agreement from the data subject

Cooke&Arkwright

Responsibility of GDPR

The responsibility of the Firms GDPR is the Cooke & Arkwright Board of Directors.

Their responsibilities are, but not limited to:

- Keeping the company updated about data protection responsibilities, risks and issues
- Reviewing all data protection procedures and policies on a regular basis
- Arranging data protection training and advice for all staff members and those included in this policy
- Checking and approving with third parties that handle the company's data any contracts or agreement regarding data processing

If you have any questions, enquiries or a subject access request regarding Cooke & Arkwright GDPR policies, please write to:

Andrew Gardner (Managing Director)
Cooke & Arkwright
7-8 Windsor Place
Cardiff
CF10 3SX

Or email: andrew.gardner@coark.com

As the GDPR regulation states, we will respond to your request/enquiry within the stated one month period upon receipt.

Signed by: Date signed: 21/8/18.

Job Title Managing Director

Document creation date: August 2018
Next review date: August 2019