GDPR Data Protection Policy

Policy information

Organisation	Collins Chartered Accountants
Scope of policy	Collins Chartered Accountants are solely based at The Lodge, Castle Bromwich Hall, Chester Road, Castle Bromwich B36 9DE. All data processing takes place at this premises.
Policy operational date	25th May 2018.
Policy prepared by	The policy is prepared by John Collins (Partner at Collins Chartered Accountants
Date approved by Board/ Management Committee	The policy is approved by the partners.
Policy review date	24th May 2021.

Introduction

Purpose of policy	The purpose of the policy is to comply with GDPR regulations but also to protect clients, staff and the organisation.
Types of data	Collins Chartered Accountants holds personal but not sensitive data for clients. All data held is required in order to act in accordance with our engagement letter and not used or passed on for any other purpose.
Policy statement	Collins Chartered Accountants will: • comply with both the law and good practice • respect individuals' rights • be open and honest with individuals whose data is held • provide training and support for staff who handle personal data, so that they can act confidently and consistently • Notify the Information Commissioner voluntarily, even if this is not required
Key risks	The key risks are information about data getting into the wrong hands through poor security or individuals being harmed through data being inaccurate.

Responsibilities

The Board / Company Directors The Partners have overall responsibility for ensuring that the organisation complies with its legal obligations.

Data Protection Officer John Collins is the Data Protection Officer whose responsibilities include:

- Briefing the partners on Data Protection responsibilities
- Reviewing Data Protection and related policies
- Advising other staff on tricky Data Protection issues
- Ensuring that Data Protection induction and training takes place
- Notification to the ICO
- Handling subject access requests
- Approving unusual or controversial disclosures of personal data
- Approving contracts with Data Processors

Employees & Volunteers All staff and volunteers are required to read, understand and accept any policies and procedures that relate to the personal data they may handle in the course of their work.

Enforcement Strict disciplinary procedures are enforced for infringing the Data Protection and related policies.

Security

Scope Various levels of security exist within the organisation depending on the nature of the information and how it is handled.

Security measures Building – protected by an alarm system directly linked to Police. CCTV in operation around the premises.
Computers – All login are strongly password protected to each member of staff including desktops and laptops. No data is held on the desktop or laptops.
Server – Strong password protection with no access by Collins. Lansalot (outsourced IT) maintain and secure the server remotely. The server is backed up online and is provided and managed by KeepItSafe. The company only know us by name with the backup's encrypted in-transit and at-rest, using a 256-bit AES key in the UK.
Payroll – all personal information is received and sent via a secure 'Openspace' platform using IRIS payroll bureau. Payslips are sent via 'e-payslips' or 'Openspace' within IRIS payroll bureau which is all GDPR compliant.
Accounts and Tax Returns – are sent via 'Onvio' platform using Thompson Reuters Digita software. This is secure multifactor authentication in the cloud and GDPR compliant. This allows the client and Collins to send and receive documents securely.

	Email and attachments – all attachments are sent password protected. External drives – Toshiba password protected USB sticks are used by all staff that allow secure collection of data when visiting client premises. Anti-virus – ESET Endpoint Protection Advanced covers all IT held by Collins.
Business continuity	Backups of all data held on the server are taken daily and held securely (stated above). A further back up is taken daily on an external hard drive daily and held off premises.
Specific risks	External organisations may request information for items such as mortgage applications. This is only given once permission granted from the client and then sent in accordance with our procedures.

Data recording and storage

Accuracy	Information is only taken from the individual, Companies House or HMRC.
Updating	Information is reviewed on a yearly basis with the client.
Storage	As stated under security measures. Hard copies are kept in archive for the required period and then disposed using a professional shredding company. A yearly inspection and review is conducted.
Retention periods	Per ICAEW regulations, data is held for 6 years.

Right of Access

Responsibility	The Partners are responsible for ensuring that right of access requests are handled within the legal time limit which is one month
Procedure for making request	Right of access requests must be in writing to Collins. All employees must pass on anything which might be a subject access request to the appropriate person without delay.
Provision for verifying identity	Where the person managing the access procedure does not know the individual personally. ID is held for all clients on file and should be checked before handing over any information
Charging	Information is provided free of charge. However a reasonable charge maybe applied when a request is manifestly unfounded or excessive, particularly if it is repetitive. We may also charge a reasonable fee to comply with requests for further copies of the same information. The fee is based on the administrative cost of providing the information.

Procedure for granting access	If the request is made electronically, we will provide the information in a commonly used electronic format. The 'Onvio' platform allows this procedure.

Transparency

Commitment	Per the signed engagement letter Collins explains its commitment to ensuring that Data Subjects are aware that their data is being processed and • for what purpose it is being processed • what types of disclosure are likely, and • how to exercise their rights in relation to the data
Procedure	All staff are fully aware of the procedures to follow which are displayed in each department.

Lawful Basis

Underlying principles	All personal data is held purely for the purpose of performing the obligations stated within the engagement letter. This is not passed onto anyone and held securely.
Opting out	Even where the organisation is not relying on consent, it may wish to give people the opportunity to opt out of their data being used in particular ways
Withdrawing consent	The organisation may wish to acknowledge that, once given, consent can be withdrawn, but not retrospectively. There may be occasions where the organisation has no choice but to retain data for a certain length of time, even though consent for using it has been withdrawn in accordance with ICAEW and HMRC regulations.

Employee training & Acceptance of responsibilities

Induction	All employees who have access to any kind of personal data have their responsibilities outlined during their induction procedures.
Continuing training	Any data protection issues will be raised during the monthly staff meetings.