Data Protection Policy

1 Introduction

CornerStone GRG Limited (hereafter referred to as CornerStone) needs to gather and use certain information about individuals.

These can include clients, suppliers, business contacts, employees 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 as well as national and European regulations – namely the Data Protection Act 2018 (DPA 2018) and the General Data Protection Regulation (GDPR).

2 Why This Policy Exists

This data protection policy ensures CornerStone:

- Complies with data protection law and follows good practice
- Protects the rights of staff, customers, partners and visitors
- Is open about how it stores and processes individuals' data
- Protects itself and individuals from the risks of a data breach and associated consequences

3 Data Protection Law

The GDPR and the DPA 2018 are both based on the same founding principles and describe how organisations, including CornerStone, must collect, handle and store personal information.

These rules apply regardless of whether data is stored electronically, on paper or on other materials.

To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

3.1 Data Protection Principles

The GDPR is underpinned by six main principles, described in Article 5:

- **Lawfulness, fairness and transparency** – Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject
- **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

- **Data minimisation** – Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
- **Accuracy** – Personal data shall be accurate and, where necessary, kept up to date
- **Storage limitation** – Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed
- **Integrity and 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, using appropriate technical or organisational measures

Article 5 adds another criterium:

- **Accountability** – The controller shall be responsible for, and be able to demonstrate compliance with the GDPR

3.2 Changes to Previous Data Protection Laws under the GDPR

Under the new GDPR and the DPA 2018, organisations must receive explicit consent from their customers for their personal information to be transferred outside of the European Economic Area (EEA). The GDPR can still hold a company liable even after data has been transferred to another country. These changes mean that companies must consider the impact the GDPR could have on their international data transfers.

4 People, Risks and Responsibilities

4.1 Policy Scope

This policy applies to:

- The head office of CornerStone
- All branches of CornerStone
- All of CornerStone's staff and senior management
- All contractors, suppliers and other people working on behalf of CornerStone
- All service providers using items of personal data provided by CornerStone or its employees. These include pension providers, certification and insurance schemes or background vetting companies, among others
- All of CornerStone's clients

It applies to all data that the company holds relating to identifiable individuals, even if that information technically falls outside of the DPA 2018 and the GDPR. This can include:

- **Personal Information** – Names of individuals, postal addresses, email addresses, telephone numbers, application forms and references, identity and residency information, contracts of employment and any amendments to it, correspondence with or about employees, for example letters about a pay rise or letters to mortgage company confirming the salary, information needed for payroll, benefits and expenses purposes, contact and emergency contact details, records of holiday, sickness and other absence; information needed for equal opportunities monitoring policy; and records relating to career history, such as training records, appraisals, certifications and degrees, vetting information, other performance measures and, where appropriate, disciplinary and grievance records
- **Special Category Information** – CornerStone does not normally process special categories of information relating to racial or ethnic origin, political opinions, religious and philosophical beliefs, trade union membership, biometric data or sexual orientation. CornerStone, however, may keep information relating to staff members' health, which could include reasons for absence and GP reports and notes. This information will be used in order to comply with CornerStone's health and safety and occupational health obligations, and to administer and manage statutory and company sick pay

4.2 Data Protection Risks

This policy helps to protect CornerStone and individuals linked to the Company, including members of staff, contractors, suppliers, clients and guests, from some very real data security risks:

- Breaches of confidentiality or loss of information. For instance, information being given out inappropriately
- Failing to offer choice. For instance, all individuals should be free to choose how the company uses data relating to them and to give their consent when it is applicable.
- Reputational damage. For instance, the company could suffer if hackers successfully gained access to sensitive data

4.3 Responsibilities

Everyone who works for or with CornerStone has some responsibility for ensuring data is collected, stored and handled appropriately.

Each team that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

However, these people have key areas of responsibility:

- The board of directors is ultimately responsible for ensuring that CornerStone meets its legal obligations
- The Data Controller is responsible for:
  - Keeping the board updated about data protection responsibilities, risks and issues
  - Reviewing all data protection procedures and related policies, in line with an agreed schedule
  - Arranging data protection training and advice for the people covered by this policy
  - Handling data protection questions from staff and anyone else covered by this policy
  - Dealing with requests from individuals to consult the data CornerStone holds about them (also called 'subject access requests')
  - Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data
  - Publishing and updating the company's privacy notice
  - Conducting Data Protection Impact Assessments (DPIA) on a regular basis when and where it is applicable
  - Defining the purpose, limitation and methods of processing data in the organisation in collaboration with senior management and in accordance with the GDPR's and the DPA 2018's aforementioned principles
  - Monitoring and act on any changes in data protection regulation
- The Technical Director of CornerStone is responsible for:
  - Ensuring all systems, services and equipment used for storing data meet acceptable security standards
  - Performing regular checks and scans to ensure security hardware and software is functioning properly
  - Evaluating any third-party services that the company is considering using to store or process data. For instance, cloud computing services
  - Monitor and act on any changes in information security and threat detection to ensure the appropriate protection of personal information within the organisation

- The Data Controller is responsible for:
    - Approving any data protection statements attached to communications such as emails and letters
    - Addressing any data protection queries from journalists or media outlets like newspapers
    - Where necessary, working with other staff to ensure marketing initiatives abide by data protection principles

5 General Staff Guidelines

- The only people able to access data covered by this policy should be those who need it for their work exclusively
- Data should not be shared informally. When access to confidential information is required, employees can request it formally from their line managers in writing
- CornerStone will provide training and regular updates to all employees to help them understand their responsibilities when handling data
- Employees should keep all data secure, by taking sensible precautions and following the guidelines below
- In particular, strong passwords must be used and they should never be shared
- Personal data should not be disclosed to unauthorised people, either within the company or externally. Inappropriate disclosure of personal data could result in grave consequences for the data subjects and for CornerStone
- Data should be regularly reviewed and updated if it is found to be out of date. If no longer required, it should be deleted and disposed of
- Employees should request help from their line manager or the data protection officer if they are unsure about any aspect of data protection:
    - Under the GDPR and the DPA 2018, individuals have a number of rights with regard to their personal data. They have the right to request from us access to and rectification or erasure of your personal data, the right to restrict processing, object to processing as well as in certain circumstances the right to data portability

- If individuals have provided consent for the processing of their data, they have the right (in certain circumstances) to withdraw that consent at any time which will not affect the lawfulness of the processing before consent was withdrawn
- Individuals have the right to lodge a complaint to the Information Commissioner's Office (ICO) if they believe that CornerStone has not complied with the requirements of the GDPR or DPA 2018 with regard to their personal data
- Individuals (including staff, sub-contractors and clients) have the right and the duty to report any security and data breaches upon their identification

6 Data Storage

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the IT manager or Data Controller.

When data is stored on paper, it should be kept in a secure place where unauthorised people cannot see it.

These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:

- When not required, the paper or files should be kept in a locked drawer or filing cabinet
- Employees should make sure paper and printouts are not left where unauthorised people could see them, like on a printer or on desks
- Data printouts should be shredded and disposed of securely when no longer required
- When data is stored electronically, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts
- Data should be protected by strong passwords that are changed regularly and never shared between employees
- If data is stored on removable media (like a CD or DVD), these should be kept locked away securely when not being used
- Data should only be stored on designated drives and servers and should only be uploaded to an approved cloud computing services and it should ideally not be saved directly to laptops or other mobile devices like tablets or smart phones when it is not essential
- Servers containing personal data should be sited in a secure location, away from general office space

- Data should be backed up frequently. Those backups should be tested regularly, in line with the company's standard backup procedures
- All servers and computers containing data should be protected by approved security software and a firewall
- Items of personal data should only be stored and processed by CornerStone as long as necessary in accordance with CornerStone's legitimate interests and legal base

7 Data Use

Personal data is of no value to CornerStone unless the business can make use of it. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft:

- When working with personal data, members of staff and sub-contractors should ensure their computers are always locked when left unattended
- Personal data should not be shared informally. In particular, it should never be sent by email, as this form of communication is not secure
- Data must be encrypted before being transferred electronically. The Technical Director can explain how to send data to authorised external contacts
- Personal data should never be transferred outside of the EEA, unless authorised by a senior manager
- Employees should not save copies of personal data to their own computers. Always access and update the central copy of any data
- Members of staff and sub-contractors should never process data on unapproved devices
- Personal data should be stored and used by CornerStone as long as necessary, and it should be deleted thereafter

8 Data Accuracy

The law requires CornerStone to take reasonable steps to ensure data is kept accurate and up to date.

The more important it is that the personal data is accurate, the greater the effort CornerStone should put into ensuring its accuracy.

It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

- Data will be held in as few places as necessary. Staff should not create any unnecessary additional data sets or keep local copies of personal data
- Staff should take every opportunity to ensure data is updated. For instance, by confirming client's details when they call
- CornerStone will make it easy for data subjects to update the information CornerStone holds about them
- Data should be updated as inaccuracies are discovered. For instance, if a customer can no longer be reached on their stored telephone number, it should be removed from the database
- It is the marketing/commercial manager's responsibility to ensure marketing databases are checked against industry suppression files every six months

9 Subject Access Requests

All individuals who are the subject of personal data held by CornerStone are entitled to:

- Ask what information the company holds about them and why
- Ask how to gain access to it
- Be informed how to keep it up to date
- Be informed how the company is meeting its data protection obligations

If an individual contacts the company requesting this information, this is called a subject access request.

Subject access requests from individuals should be made by email, addressed to the Data Controller at datacontroller@cornerstonegrg.co.uk. The Data Controller can supply a standard request form, although individuals do not have to use this.

CornerStone will provide a copy of the information free of charge. However, CornerStone can charge a £10 fee or refuse to respond when a request is manifestly unfounded or excessive, particularly if it is repetitive. CornerStone will also charge a £10 fee to comply with requests for further copies of the same information.

The Data Controller will aim to provide the relevant data within 30 days. CornerStone will be able to extend the period of compliance by a further two months where requests are complex or numerous. If this is the case, CornerStone will inform the originator of the subject access request within one month of the receipt of the request and explain why the extension is necessary.

The Data Controller will always verify the identity of anyone making a subject access request before handing over any information.

9.1 Disclosing Data for Other Reasons

In certain circumstances, the DPA 2018 and the GDPR allow personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances, CornerStone will disclose requested data. However, the Data Controller will ensure the request is legitimate, seeking assistance from the board and from the company's legal advisers where necessary.

9.2 Providing Information

CornerStone aims to ensure that individuals are aware that their data is being processed and that they understand:

- What types and items of data are being processed
- How the data is being used
- How to exercise their rights

To these ends, the company has a privacy statement and a privacy notice, setting out how data relating to individuals is used by the company.