General Data Protection Regulation (GDPR) Policy

Introduction

The Company needs to gather, retain, and use certain information about their customers, suppliers, business contacts, employees and other people the organisation has a relationship with or may need to contact.

This policy sets out how personal data must be collected, handled, and stored in order to meet the Company's data protection standards and to comply with the law.

1. Purpose

The Data Protection Policy ensures the following objectives are met by the organisation:

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

It should be noted that until 25 May 2018, the Company shall remain subject to the requirements of the Data Protection Act, 1998 ('DPA'). From 25 May 2018, the Company will be subject to the GDPR and any other Data Protection legislation applicable in the United Kingdom.

2. Scope

This policy relates to all personal information processed by, or on behalf of the Company and covers:

- The head office and all branches, including subsidiaries of the business.
- All employees
- All contractors, suppliers and other people working on behalf of the Company.

The formats in which personal data is handled can range from electronic, hard-copy, CCTV, and voice recording, to spoken forms of communication.

Personal data is any information that can be attributed to an identifiable individual, such as names, e-mail addresses and phone numbers.

Sensitive personal data or 'special category data' includes disability status, sexual orientation, sex life, ethnicity, medical information (both physical and mental health), political, philosophical, and religious opinions/beliefs, and details of criminal convictions or allegations.

This category of data requires enhanced security measures such as encryption, password protection and stricter electronic as well as manual access controls (e.g., a locked filing cabinet).

Other categories of data also require enhanced protection, such as bank/financial details and national insurance numbers.

This policy also applies to de-identified (pseudonymised) personal data, where individuals can be re-identified from other information.

3. Rights

A 'data subject' is an individual to whom personal data relates and every data subject has the following qualified rights:

- The right to rectification should information held be inaccurate or incomplete.
- The right to restrict processing and/or erasure of personal data.
- The right to data portability.
- The right to object to processing.
- The right to object to automated decision making and profiling.
- The right to complain to the Information Commissioner's Office (ICO)
- The right to ask what information the Company holds about them and why.

Individuals can submit a written request to access personal data that the Company may hold about them. This is called a 'Subject Access Request' and can be sent via e-mail to gdpr@agilico.co.uk and addressed to the Company's Data Controller. In response to this request, the Company's Data Controller:

- Can supply a standard request form, however individuals do not have to use this.
- Will always verify the identity of anyone making a 'subject access request' prior to fulfilling the request.
- Will aim to provide the relevant data within 14 days of verifying the individual's identity.

If a request is manifestly unfounded or excessive, particularly if it is repetitive, the Company will withhold the right to impose a reasonable charge to fulfil the request.

4. Obligations

In order to comply with Government legislation, information must be collected and used fairly, stored securely and not disclosed to any other person unlawfully. This is captured in the data protection principles set out in the GDPR and those handling personal data must adhere to these principles.

Personal data shall be:

- Obtained, processed, and used fairly, lawfully, and transparently.
- Collected for specified, explicit and legitimate purposes and not processed for any other purpose.
- Adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.
- Accurate and where necessary kept up to date.
- Kept for no longer than is necessary.
- Protected by appropriate security measures to prevent loss or unauthorised access.

The personal data that is requested at the time of sale or service request, will purely be used to fulfil the request. Data Controllers ensure that guidelines are in place for personal data to only be used for the intentions set out to the data subject at the time of the request.

In addition, personal data should not be transferred outside of the European Economic Area. In cases where this may be necessary, advice of the Data Controller is sought.

5. Retention

When it is no longer required for the purpose it was originally collected, the Company destroys or archives personal data from its systems. The type of information held will determine the length of time the data is kept.

Below is a list of non-exhaustive examples of situations where data may be retained:

- For a specific time-period to comply with financial or other regulations.
- To comply with legal requirements, such as Tax or Employment law.
- Indefinitely retain certain data to support the services we offer e.g., unsubscribing from marketing communications or opting out of certain types of processing.
- Keeping personal data for as long as someone is actively engaged with our business.
- Exceptions may apply to the processing for historical or statistical purposes.

6. Data Protection

When data is stored on paper, it is 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 a specific reason:

- When not required, the paper or files are kept in a locked drawer or filing cabinet.
- The Company operates a ‘clear desk’ policy which ensures data is not left on view.
- Through use of a secure release print management system, documents are released from the printer only when ready for collection.
- Each regional office has a shredding facility to securely destroy documents of a sensitive nature that are no longer required.

When data is stored electronically, it is protected from unauthorised access, accidental deletion, and malicious hacking attempts. Therefore, the business ensures the following:

- A strong password policy is in place.
- Data stored on removable media is locked away securely when not being used.
- Data is only stored on designated drives and servers.
- Servers containing personal data are sited in a secure location at the Company’s head office.
- In the case of SaaS systems, data is only ever uploaded to approved cloud computing services.
- Data is backed up frequently. Those backups are tested regularly, in line with the Company’s standard backup procedures.
- All mobile devices are encrypted for additional data security.

- All servers and computers containing data are protected by approved security software and a firewall. We engage a third party to conduct regular IT security penetration testing.
- Software patches are implemented in line with software vender recommendations.
- The business has assigned Data Controllers to specifically manage personal data in specified systems, who will determine 'how' and 'what' the data should be used for. These Data Controllers have extensive knowledge about the systems they are responsible for and are actively working with the IT department to ensure that only relevant Data Processors have access to their systems.

7. Data Accuracy

The law requires the Company 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 the organisation will 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.

- Employees take every opportunity to ensure data is accurately updated.
- The business will ensure a simplified process is established for data subjects to update the information it holds about them.
- Data is updated as inaccuracies are discovered.
- The Head of Marketing will ensure marketing databases are checked against industry suppression files every six months.

8. Personal Data Breaches

Should an employee become aware that personal data is lost, misused, compromised, or stolen, it is their responsibility to immediately notify the Company's internal IT Helpdesk team (a division of the Technology Services department). This can be done by phone or e-mail to gdpr@agilico.co.uk. This includes, for example, the loss of a laptop or Company mobile phone.

Where necessary, the Company's Data Controller will report breaches to the Information Commissioner's Office (ICO) and notify all individuals affected.

9. Responsibilities

Everyone who works for or with Agilico has some responsibility for ensuring data is collected, stored and handled appropriately. Each team that handles personal data ensures that it is handled and processed in line with this policy and data protection principles.

However, these people have key areas of responsibility:

a) The Board of Directors is ultimately responsible for ensuring that the organisation meets its legal obligations.

b) The Company Data Controller and Head of Technology Services 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.
- Working with the Head of HR to arrange the relevant data protection training and advice for the people covered by this policy.
- Handling data protection questions from employees and any other individuals who may be covered by this policy.
- Dealing with requests from individuals to access the data that the Company may hold about them (also referred to as 'subject access requests').
- Checking and approving any contracts or agreements with third parties that may handle the Company's sensitive data.
- 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 service, the Company may consider using to store or process data, such as cloud computing services.

c) The Chief Marketing Officer 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 colleagues to ensure marketing initiatives abide by data protection principles.

10. Providing Information

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

- How the data is being used
- How to exercise their rights

To support this objective, the Company has a privacy statement, setting out how data relating to individuals is used by the Company. This is available on request; however, a version of this statement is also available on the Company's website http://www.agilico.co.uk.

Document Policy Change

This policy can be changed at any time and will be reviewed periodically.

Latest Revisions

Revision 1.2 (01/04/2021)

Understanding this Document

If an employee is unsure about any of the terms listed within this document and need clarity on any aspect, please raise a private query to the HR department.