GDPR Data Protection Policy

Introduction

The Company needs to gather and use certain information about individuals. These can include customers, 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 — and to comply with the law.

Why this policy exists

This data protection policy ensures the Company:

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

Data protection law

The Data Protection Act 2018 and General Data Protection Act 2021 describes how organisations — including the Company— 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.

The Data Protection Act is underpinned by eight important principles. These say that personal data must:

1. Be processed fairly and lawfully
2. Be obtained only for specific, lawful purposes
3. Be adequate, relevant and not excessive
4. Be accurate and kept up to date
5. Not be held for any longer than necessary
6. Processed in accordance with the rights of data subjects
7. Be protected in appropriate ways
8. Not be transferred outside the European Economic Area (EEA), unless that country or territory also ensures an adequate level of protection.

People, risks and responsibilities

Policy scope

This policy applies to:

- Head office
- All branches and associated offices

- All staff and volunteers
- All contractors, suppliers and other people working on behalf of the Company
- It applies to all data that the company holds relating to identifiable individuals, even if that information technically falls outside of the Data Protection Act 2018. This can include:
- Names of individuals
- Postal addresses
- Email addresses
- Telephone numbers
- plus, any other information relating to individuals

Data protection risks

This policy helps to protect the Company from some very real data security risks, including:

- Breaches of confidentiality. 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.
- Reputational damage. For instance, the company could suffer if hackers successfully gained access to sensitive data.

Responsibilities

Everyone who works for or with the Company 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 the Company meets its legal obligations.
- Where appointed, The Date Protection Officer, 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 see the data the Company 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.

The General Manager, 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, the company is considering using to store or process data. For instance, cloud computing services.
- Ensure all employees complete the GDPR Consent Form.

The Operations Director, 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.

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

General staff guidelines

- The only people able to access data covered by this policy should be those who need it for their work.
- Data should not be shared informally. When access to confidential information is required, employees can request it from their line managers.
- The Company will provide training 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.
- 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.
- 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.

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.
- 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 service.
- 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.
- Data should never be saved directly to laptops or other mobile devices like tablets or smart phones.
- All servers and computers containing data should be protected by approved security software and a firewall.

Data use

We use personal data for the following purposes:

Receiving services or product

We process data in relation to our suppliers and their staff as necessary to receive the services, e.g. where a supplier is providing us with a service, we will process personal data about those individuals who are providing the services.

Providing professional services or products to clients

Where a supplier is helping us to deliver services to a client, we process personal data about the individuals involved in providing the services in order to administer and manage our relations with suppliers and the relevant individuals and to provide such services to our clients.

Administering, managing and developing our business and services

We process personal data in order to run our business, including:

- Managing our relationship with suppliers.
- Developing our businesses and services (such as identifying client needs and improvements in service delivery).
- Hosting or facilitating the hosting of events

Security, quality and risk management activities

We have security measures in place to protect our and our clients' information (including personal data), which involves detecting, investigating and resolving security threats. Personal data may be processed as part of the security monitoring that we undertake, e.g. automated scans to identify harmful emails. We have policies and procedures in place to monitor the quality of our services and manage risks in relation to our suppliers. We collect and hold personal data as part of our supplier contracting procedures. We monitor the services provided for quality purposes, which may involve processing personal data.

Complying with any requirement of law, regulations or professional body of which we are members

We are subject to legal, regulatory and professional obligations. We need to keep certain records to demonstrate that our services are provided in compliance with those obligations and those records may contain persona data.

Personal data is of no value to the Company 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, employees should ensure the screens of their computers are always locked when left unattended.
- Personal data should not be shared informally. It should never be sent by email, as this form of communication is not secure.

- Data must be encrypted before being transferred electronically. The IT manager can explain how to send data to authorised external contacts.
- Personal data should never be transferred outside of the European Economic Area.
- Employees should not save copies of personal data to their own computers. Always access and update the central copy of any data.

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 Company 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.
- Staff should take every opportunity to ensure data is updated. For instance, by confirming a
- customer's details when they call.
- The Company will make it easy for data subjects to update the information it holds about them. For instance, via the company website.
- 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 manager's responsibility to ensure marketing databases are checked against
- industry suppression files every six months.

Subject access requests

All individuals who are the subject of personal data held by the Company 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 and this email address can be provided by your line manager. The data controller can supply a standard request form, although individuals do not have to use this.

Individuals will not be charged for the subject access request. The data controller will aim to provide the relevant data within 14 days.

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

Disclosing data for other reasons

In certain circumstances, the Data Protection Act allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances, the Company 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.

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

Data Breach

A personal data breach is a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This will include breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

It is a security incident that has affected the confidentiality, integrity or availability of personal data. Whenever a security incident takes place, it should be quickly established whether a personal data breach has occurred and, if so, the Company will promptly take steps to address it, including informing the Information Commissioner's Office (ICO) if required.

The ICO must be informed if the breach has resulted in a risk to people's rights and freedoms; if this is unlikely then it does not have to be reported. However, if the breach has not been reported then the Company should be able to justify this decision.

In assessing if a data breach has created a risk to people's rights and freedoms then Recital 85 of the GDPR should be consulted:

"A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned."

Actions that the Company may take following a data breach may include:

- Training.
- Disciplinary action.
- Dismissal.

The following process should be followed in circumstances where an employee becomes aware of a data breach:

1. The Data Breach is to be reported to the Data Protection Manager (DPM).
2. The DPM will take immediate action to contain the breach.
3. The DPM will begin completion of the data breach document log.
4. The DPM will ensure that any remedial actions are identified and carried out.
5. The DPM will inform the Managing Director of the data breach in a timely manner.

The data breach document log is to be signed off by both the DPM and the Managing Director on completion of the review into the data breach.

This is available on request. A version of this statement is also available on the www.Gencocs.co.uk.
Genco reserves the right to amend and update this Policy at any time.

John Roberts

Director

Dated: February 2023