# Data Protection Policy

**23-05-2018**

**Context and overview**

**Key details**

| | |
|---|---|
| • Policy prepared by: | D.Witts-Price |
| • Approved by board / management on: | 23rd May 2018 |
| • Policy became operational on: | 23rd May 2018 |
| • Next review date: | Monthly until fully compliant |

**Introduction**

The SGD Group Ltd (SGD) 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 Article 1,2**

This data protection policy ensures SGD:

• 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 Article 1,2,3,5,6,25,40**

The Data Protection Act 1998 describes how organisations including SGD 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:

• The head office of SGD

• All branches and trading names of SGD

• All staff of SGD

• All contractors, suppliers and other people working on behalf of SGD.

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 1998. 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 SGD 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 SGD 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 **Directors** are ultimately responsible for ensuring that SGD meets its legal obligations.

• The **Data Protection Officer, David Witts-Price**, **(Article 24,37,41)** is responsible for:

o Keeping the board updated about data protection responsibilities, risks and issues.

o Reviewing all data protection procedures and related policies, in line with an agreed schedule.

o Arranging data protection training and advice for the people covered by this policy.

o Handling data protection questions from staff and anyone else covered by this policy.

o Dealing with requests from individuals to see the data SGD holds about them (also called 'subject access requests').

o Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data.

• The **IT Manager, Paul Corcoran,** is responsible for:

o Ensuring all systems, services and equipment used for storing data meet acceptable security standards.

o Performing regular checks and scans to ensure security hardware and software is functioning properly.

o Evaluating any third-party services the company is considering using to store or process data. For instance, cloud computing services.

• The **Marketing Manager, David Witts-Price,** is responsible for:

o Approving any data protection statements attached to communications such as emails and letters.

o Addressing any data protection queries from journalists or media outlets like newspapers.

o Where necessary, working with other staff to ensure marketing initiatives abide by data protection principles.

**General Staff Guidelines and Data Security Article 32,39**

• 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.

• SGD 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.

• 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.

• 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 Collection Article 7,8,9,13**

SGD collects data only for its legitimate business obligations. The data is the property of the client and can be deleted at any time on a written request from the client. SGD terms and conditions of sale reflect that the individual's data is their own and only legitimate information to carry out our legitimate business is stored. Consent is shown by accepting our terms and conditions.

CCTV image collection. SGD has installed on its premises various CCTV devices for client display and training as well as the security of the building. These images are kept for a maximum of 3 months prior to deletion and are available to the police on an official request and by members of the public on a written request (subject to approval by the Data Protection Officer) and subject to a reasonable charge.

CCTV installation by SGD Security Systems. The design and security of the system is subject to an on-site "privacy impact assessment" and any unreasonable request that breaches GTDPR guidelines will be refused by the company. Once installed the protection of data is the client's GDPR responsibility

No data is collected on children

No data is collected on “special categories”

**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 services.

• 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 Article 10,11,22,27,37,44,45,46,47,48,49**

Personal data is of no value to SGD 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. 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 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.

• Employee data is used to discriminate against employing people relating to criminal convictions and offences

• SGD does not process data that does not require identification.

• SGD does not process "automated individual decision-making, including profiling".

• SGD will not transfer information outside the European Union or vetted contractors

**Data Breach Article 33,34,38**

All employees of SGD are required within their terms of contract to;

• Bring to the attention of their line manager any obvious breach of client, employee or supplier data

• Bring to the attention of their line manager any potential breach of client, employee or supplier data including possible external hacking

• Managers must relay the information from employees to the Company's data Protection Officer and to a Company director.

• The Company's Data Protection Officer in collaboration with the Director and relevant management team are responsible for immediate corrective action to notify the person whose data has been accessed as well as statutory notification under GDPR. Corrective action for the disclosure and remedial action must be minuted.

.

**Privacy Impact Assessments Article 35, 14**

SGD carries out "privacy impact assessments "on the data stored or created by the business;

• HR information is stored in a locked area and only available to those directly responsible for HR

• Client's data is not released to third parties other than those covered by these regulations and necessary for the Company's execution of its contractual obligations

• SGD operates within the security industry to the highest standards and views client's data as privileged and confidential information and will not release this information to marketing companies or third-party data acquisition businesses.

SGD does not access or obtain individual's data from third parties

**Data accuracy Article 16,18**

The law requires SGD 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 SGD 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.

• SGD will make it easy for data subjects to update the information SGD 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.

**Subject access requests and deletion of records Article 12, 13,15,17, 19,20,21**

All individuals who are the subject of personal data held by SGD 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 mike@SGD .co.uk. The data controller can supply a standard request form, although individuals do not have to use this.

Individuals will be charged £10 per 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.

Individuals can at any stage "object" to having their data stored and request that it is destroyed

**Records of Processing Activities Article 12, 26, 28, 29,30,31,35,39**

SGD maintains the following table to record the Company's processing activities. All processing activities are done within the European Union. Any shared data will be subject to GDPR with a vetted third party with proof of compliance. All new data processed or new means of processing will be evaluated by the data Protection Officer to assess its impact on data security. If the Data Protection Officer feels that there is a high risk then he/she will consult the supervisory authority.

| Type Of Data | Storage Method | Access / Security | Deletion | Storage Duration | Responsibility | Purpose of Processing |
|---|---|---|---|---|---|---|
| HR Files | Paper in a locked filing cabinet in a secure restricted access room | HR and Director | Upon written request from person | Indefinite | Data Protection Officer | Legitimate Business Activity |
| Customer Information | Mentor's CASH software on our Servers. | Secure firewalled server with encryption, and secure restricted access room. Company computers with firewall and passwords | Upon written request from person, and in line with HMRC, NSI, BAFE and MLA criteria | 5 years after cancellation | Data Protection Officer | Legitimate Business Activity |
| Remote Monitoring Customer Information | Mentor's CASH software on our Servers. | Secure firewalled server with encryption, and secure restricted access room. Alarm Receiving Centre and Video Receiving Centre | Upon written request from person, and in line with HMRC, NSI, BAFE and MLA criteria | 7 years | Data Protection Officer & Monitoring Station Data Protection Officer | Legitimate Business Activity |
| CCTV Images | Hard drive on recording device | Password and firewall protection in a secure area | Rolling recordings maximum of three months | Rolling, maximum 3 months | Data Protection Officer | Legitimate Business Activity |

| | | | | | | |
|---|---|---|---|---|---|---|
| Accounts Data | Sage software on our servers with back up. | Secure firewalled server with encryption, and secure restricted access room. Company computers with firewall and passwords | Upon written request from person, and in line with HMRC, NSI, BAFE and MLA criteria | 7 years | Data Protection Officer | Legitimate Business Activity |
| Credit Card Details | PCI compliant, no card details are stored after processing | Processed via a PDQ or online via a PCI compliant secure website | Not applicable, no details are retained | Not applicable | Data Protection Officer | Legitimate Business Activity |
| Working Files For Contracts | Paper within admin office | Restricted access, physical protection | Upon completion of the job the paperwork is scanned into the CASH system and then shredded | Duration of work being done | Data Protection Officer | Legitimate Business Activity |
| Computers and Laptops | limited storage on local system. Secure remote access to office | Secure password protected access with physical protection | Upon written request from person, and in line with HMRC, NSI, BAFE and MLA criteria | 7 years | Data Protection Officer | Legitimate Business Activity |
| PDAs And Phones | limited storage on local system. Secure remote access to office. CASH Software on PDA/Phone is encryted and cannot be copied from the device or printed out | Secure password protected access with physical protection | Upon written request from person, and in line with HMRC, NSI, BAFE and MLA criteria | 7 years | Data Protection Officer | Legitimate Business Activity |

**Certification Article 42,43**

SGD has advised its certificating body the NSI that it would seek third party certification if they would take on the role.

**Disclosing data for other reasons Article 23,31**

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, SGD 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 Article 12**

SGD 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.

[This is available on request. A version of this statement is also available on the company's website.]

**Articles 50 -99**

SGD as a data holder and not supervisory authority is subject to but not part of these articles