goSystem

goSystem Solutions Limited

Data Protection & Handling Policy

goSystem Solutions Limited 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.

1 Data Protection Law

1.1 The Data Protection Act 2018 describes how organisations - including goSystem Solutions Limited - must collect, handle and store personal information.

1.2 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.

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

(a) Be processed fairly and lawfully
(b) Be obtained only for specific, lawful purposes
(c) Be adequate, relevant, and not excessive
(d) Be accurate and kept up to date
(e) Not be held for any longer than necessary
(f) Processed in accordance with the rights of data subjects
(g) Be protected in appropriate ways
(h) Not be transferred outside the European Economic Area (EEA), unless that country or territory also ensures an adequate level of protection

2 People, Risks and Responsibilities

2.1 This policy applies to:

(a) The head office of goSystem Solutions Limited
(b) All branches of goSystem Solutions Limited
(c) All contractors, suppliers and other people working on behalf of goSystem Solutions Limited

2.2 This policy 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:

(a) Names of individuals
(b) Postal addresses
(c) Email addresses
(d) Telephone numbers
(e) Any other information relating to individuals

goSystem

3 Data protection risks

3.1 This policy helps to protect goSystem Solutions Limited from some very real data security risks, including:

(a) **Breaches of confidentiality**
For instance, information being given out inappropriately.

(b) **Failing to offer choice**
For instance, all individuals should be free to choose how the company uses data relating to them.

(c) **Reputational damage**
For instance, the company could suffer if hackers successfully gained access to sensitive data

4 Responsibilities

4.1 Everyone who works for or with goSystem Solutions Limited has some responsibility for ensuring the data is collected, stored, and handled appropriately.

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

4.3 The board of directors is ultimately responsible for ensuring that goSystem meets its legal obligations regarding data handling and protection.

4.4 The Data Protection Officer (DPO) is responsible for:

(a) Keeping the board updated about data protection responsibilities, risks, and issues.

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

(c) Arranging data protection training and advice for the people covered by this policy.

(d) Handling data protection questions from staff and anyone else covered by this policy.

(e) Dealing with requests from individuals to see the data goSystem holds about them (also called "Subject Access Requests")

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

4.5 The Operations Director is responsible for:

(a) Ensuring all systems, services and equipment used for storing data meets acceptable security standards

(b) Performing regular checks and scans to ensure security hardware and software is functioning properly

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

4.6 The Sales Director is responsible for:

(a) Approving any data protection statements attached to communications such as emails and letters

(b) Addressing any data protection queries from journalists or media outlets such as newspapers.

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

goSystem

5 General staff guidelines

The only people able to access data covered by this policy should be those who need it for their work.

(a) Data should not be shared informally. When access to confidential information is required, employees can request it from their line managers.

(b) goSystem will provide training to all employees to help them understand their responsibilities when handling data.

(c) Employees should keep all data secure, by taking sensible precautions and following the guidelines outlined in this policy

(d) Strong passwords must be used, and they should never be shared.

(e) Personal data should not be disclosed to unauthorised people, either within the company or externally.

(f) 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.

(g) Employees should request help from their line manager or the data protection officer if they are unsure about any aspect of data protection.

6 Data storage

6.1 When data is stored on paper, it should be kept in a secure location where unauthorised personnel cannot access or see it.

(a) When not required, the paper or files should be kept in a locked drawer or filing cabinet.

(b) Employees should make sure paper and printouts are not left where unauthorised personnel could see them.

(c) Data printouts should be shredded and disposed of securely when no longer required.

6.2 When data is stored electronically, it must be protected from unauthorised access, accidental deletion, and malicious hacking attempts

(a) Data should be protected by strong passwords that are changed regularly and never shared between employees

(b) Where possible the data should be protected using two-factor authentication

(c) If data is stored on removable media, these should be kept locked away securely when not in use

(d) Data should only be stored on designated drives and servers and should be uploaded to an approved cloud computing service.

(e) Servers containing personal data should be sited in a secure location.

(f) Data should be backed up frequently. Those backups should be tested regularly, in line with the company's standard backup procedures.

(g) Data should never be saved directly to laptops or other mobile devices like tablets or smartphones.

(h) All servers and computers containing data should be protected by approves security software and a firewall.

goSystem

7 Data use

Personal data is of no value to goSystem Solutions Limited 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:

(a) When working with personal data, employees should ensure the screens of their computers are always locked when left unattended.

(b) Personal data should not be shared informally. In particular, it should never be sent by email, as this form of communication is not secure.

(c) Data must be encrypted before being transferred electronically. The IT manager can explain how to send data to authorised external contacts.

(d) Personal data should never be transferred outside of the European Economic Area.

(e) Employees should not save copies of personal data to their own computers. Always access and update the central copy of any data.

(f) When working with personal data, employees should ensure the screens of their computers are always locked when left unattended.

(g) Personal data should not be shared informally. In particular, it should never be sent by email, as this form of communication is not secure.

(h) Data must be encrypted before being transferred electronically. The IT manager can explain how to send data to authorised external contacts.

(i) Personal data should never be transferred outside of the European Economic Area.

(j) Employees should not save copies of personal data to their own computers. Always access and update the central copy of any data.

8 Data accuracy

8.1 The law requires goSystem Solutions Limited 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 goSystem Solutions Limited should put into ensuring its accuracy.

8.2 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.

(a) Data will be held in as few places as necessary. Staff should not create any unnecessary additional data sets.

(b) Staff should take every opportunity to ensure data is updated. For instance, by confirming a customer's details when they call.

(c) goSystem Solutions Limited will make it easy for data subjects to update the information goSystem Solutions Limited holds about them. For instance, via the company website.

(d) 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.

(e) It is the marketing manager's responsibility to ensure marketing databases are checked against industry suppression files every six months.

goSystem

9 Subject access requests

9.1 All individuals who are the subject of personal data held by goSystem Solutions Limited are entitled to:

(a) Ask what information the company holds about them and why.

(b) Ask how to gain access to it.

(c) Be informed how to keep it up to date.

(d) Be informed how the company is meeting its data protection obligations.

9.2 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 privacy@gosystem.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.

10 Disclosing data for other reasons

10.1 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, goSystem Solutions Limited 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.