Data Protection Policy

Table of Contents

Data Protection Policy Statement.

Grosvenor Services 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 the personal data must be collected, processed and stored to meet the companies' data protection standards and to comply with the law.

Why this policy exists

This data protection policy insures that Grosvenor Services complies with GDPR and any national requirements of the countries in which we operate, and follows good practice,

1. *Protects the rights of staff, customers and partners.*
2. *Is open about how it stores and processes individuals' data.*
3. *Protect itself from the risks of a data breach*

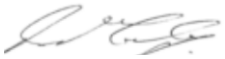
Data protection law and the general data protection regulations describes how we must collect handle process and protect and store personal information.

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

To comply with the law personal information must be collected and used fairly, stored safely and not disclosed unlawfully. GDPR is underpinned by six important principles.

1. *processed lawfully, fairly and in a transparent manner in relation to individuals*
2. *collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes*
3. *adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed*
4. *accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay*
5. *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; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and*
6. *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*

This policy will be reviewed on an annual basis or as changes in the law or our business dictates.



Bernard McCauley
Group Managing Director.

Policy scope.

This policy applies to;

The head office of Grosvenor Services all branches of Grosvenor Services all staff and volunteers of Grosvenor services all contractors, suppliers and other people working on behalf of Grosvenor Services.

It applies to all data that the company holds relating to personal and sensitive personal information relating to an identifiable natural person.

Sensitive Personal Data

Definition under the DPA: *personal data consisting of information as to:*

(a) The racial or ethnic origin of the data subject;
(b) Political opinions;
(c) Religious beliefs or other beliefs of a similar nature;
(d) Trade union membership
(e) Physical or mental health or condition;
(f) Sexual life;
(G) Commission or alleged commission of any offence; or
(h) Any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings.

Personal Data

Is any information relating to an identified or identifiable natural person?
This can include;

1. Names of individuals
2. Postal addresses
3. Email addresses
4. Telephone numbers
5. 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:

1. Breaches of confidentiality, for instance information being given out inappropriately.

2. Failing to offer choice, for instance all individual should be free to choose as to how the company uses data relating to them.

3. Reputational damage, for instance the company could suffer if hackers successfully gained access to sensitive data.

Responsibilities.

All employees who have access to data have responsibility for ensuring data is collected, stored and protected, processed appropriately.

Each team that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles. The board of directors is ultimately responsible for ensuring that we meet our legal obligations.

The company has appointed a **data protection steering committee.**

The steering committee is chaired by:

1. George Parish, Business Improvement Director and consists of.
2. Barry McGrane finance Director.
3. Brian Solan Head of HR.
4. Tom Rossiter Head of IT.

Data Controller

Background

Pursuant to Article 37 of GDPR we note that there is a requirement for a controller and processor to designate a Data Protection Officer (DPO) in any case where:

a. The data processing is carried out by a public authority;

b. The core activities of the controller and processor require regular and systematic monitoring of data subjects on a large scale; or

c. The core activities of the controller and processor consist of large scale processing of special categories of data and/or personal data relating to criminal convictions and offences.

Grosvenor Services has considered the requirements of GDPR and in particular Article 37 in order to decide whether it was required to appoint a D P O. Grosvenor Services wishes to record that it has considered the matter in an appropriate manner and to record its decision.

Matters considered

In coming to a decision, Grosvenor Services, has noted the following:

- We are a private entity and not a public authority.
- Whilst certain monitoring of individuals' takes place in the context of recording our staff/employees' attendance at work and CCTV systems are used for safety and security of staff, premises and property, such monitoring is not a core activity of the business.
- The core activity of the business is the provision of facilities management and related services.
- We carry out limited processing of special category data related to staff/employee health records and information relating to criminal convictions. Such information is processed in the context of interacting with our staff/employee and for human resources purposes and for no other reason.

In this regard we note that the processing of this type of information is not a core activity of Grosvenor Services.

- We are not subject to any national or EU Law which would require the appointment of a DPO.

Conclusion

On the basis of the foregoing matters, Grosvenor Services has decided that it is not required to appoint a Data Protection Officer. The Data Protection function will be managed in Grosvenor by the appointment of a Data Protection Manager. This will be George Parish, Business Improvement Director.

The steering committee is responsible for:

1. Appointing a named person to be responsible for data protection in the business.
2. The named person for Grosvenor Services is George Parish.
3. The steering committee will be responsible for keeping the board updated about data protection responsibilities risks and issues.
4. Reviewing all data protection procedures and related policies in line with an agreed schedule.
5. Arranging ongoing training advice from people covered by this policy.
6. Handling data protection questions from anyone else covered by this policy.
7. Dealing with requests from individuals to access the data we hold about them also called 'subject access request'.
8. Checking and approving any contractual agreement with third parties where they handle the companies' data.
9. Approving any data protection statements attached to communications such as emails and letters.

Head of IT is responsible for.

1. Ensuring all systems services and equipment used for storing data meet acceptable security standards.
2. Performing regular checks and scans to ensure security hardware and software is functioning properly.
3. Evaluating any third-party services the company is considering using to store or process data for instance, cloud computing services.

Data Protection Manager

1. Data Protection Manager Addressing any data protection queries from journalists or media outlets like newspapers.
2. When necessary working with all the staff to ensure data protection principles are being applied.
3. Any subject access requests

4. Inform the ICO (UK) or Data Protection Agency (IRL) of any data protection breach.

Each department has an appointed champion who is responsible for:

1. Ensuring the policy is communicated and understood by his/her staff.
2. Ensuring that the policy and processes are applied in practice.
3. Regularly reviewing the process to ensure they are fit for purpose, and reporting back to the DPM.
4. Regularly auditing compliance
5. Dealing with offenders in a just way.

Company Guidelines

Where personal data is processed or held, the area in which its held must be secure with restricted access. Any person involved in handling personal data MUST sign a non-disclosure form. Failure to comply with the requirement could result in disciplinary proceedings.

Where legitimate access is required to data, the paper files cannot be taken from the restricted area unless the original is required in a court of law, in which case this is against a signature.

Grosvenor services operates a clean desk policy.

All files containing personal or sensitive data must be secured in a locked cabinet or file when not in use.

General staff guidelines.

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

2. Data should not be shared informally. When access to confidential information is required employees can request from their line managers.

3. We will provide training to all employees to help them understand their responsibilities when handling data.

4. Employees should keep all data secure by taking sensible precautions and following the guidelines below.

5. In particular strong passwords must be used and they should never be shared.

6. Personal data should not be disclosed to an unauthorised person either within the company or externally.

7. Data should be regularly reviewed and updated if it is found to be out of date if no longer required it should be deleted or disposed of as per the company guidelines.

8. Disposal periods are identified in appendix 1 to this policy.

9. Employee should request help from the line manager or data protection manager if they are unsure about any aspect of data protection.

Data storage and disposal.

These rules describe how and where data should be stored. Questions about storing data safely should be directed to a member of the steering committee.

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

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

1. All confidential papers containing data should be kept in a locked drawer filing cabinet.
2. Employee should make sure paper and printouts are not left where an unauthorised person could see them like on the printer.
3. Data printout should be shredded and disposed of securely when no longer required.
4. When data is stored electronically must be protected from unauthorised access accidental deletion or malicious hacking attempts
5. Data should be protected by strong passwords and changed regularly and never shared between employees.
6. If data stored on removable media like CD or DVD or memory stick it should be kept locked away securely when not being used.
7. Data must only be stored on designated drives and service and should only be uploaded on an approved cloud computing services.
8. Servers containing personal data must be cited in a secure location away from general office space and secured.
9. Data must be backed up frequently those backups should be tested regularly, in line with the company standard backup at procedures.
10. Data should never be saved directly to laptops or mobile devices like tablets or smart phones.
11. All servers or computers containing data must be protected by approved security software and the firewall.
12. Any personal data used in presentations MUST be anonymised.

Archiving

All paper based archive, should be in boxes marked, to show the content and the disposal date.
The area or buildings in which the boxes are kept MUST be secure.
Every 3 months, the person responsible, will dispose of the data either by shredding or via a third party confidential waste disposal company.
Only authorised persons (approved by head of department) may access any stored data.

Data use

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

1. When working with personal data employee should ensure the screens of the computers are always locked when left unattended.
2. Personal data MUST not be shared informally in particular it should never be sent by email as this form of communication is not secure.
3. Data must be encrypted before being transferred electronically. DISCUSSION
4. Personal data must never be transferred outside of the European Economic area.
5. Employee should not share copies of personal data from computers. Always access and update the central copy of any data.

Data accuracy.

1. The law requires us to take reasonable steps to ensure data is kept accurate and up-to-date.
2. The more important it is that personal data is accurate the greater the effort should be to ensure its accuracy.
3. Data will be held in a few places as necessary staff should not create any unnecessary additional data sets.
4. Staff should take every opportunity to ensure date is updated. For instance by confirming our customers details when they call.
5. We will make it easy for data subjects to update the information we hold about them.
6. It is the marketing manager‘s responsibility to ensure marketing databases are checked every six months

Subject access requests.

All individuals who are the subject of personal data held by us are entitled to;

1. Ask what information the company holds about them and why.
2. Ask how to get access to it.
3. Be informed how we keep it up-to-date.
4. Be informed how the company is meeting its contractual and legal obligations.

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

Subject access requests from individuals can be received by email, or addressed to the HR manager at 64c Heather road Sandyford Dublin Ireland or The HR Manager 10 Algitha Road Skegness, Lincs, UK. The manager will supply standard request forms, although this is not necessary.

The HR manager will aim to provide the relevant data within 30 days.

The HR manager will always verify the identity of anyone making subject access request before handing over the information.

Disclosing data for other reasons.

In certain circumstances the law allows personal data to be disclosed to law-enforcement agencies without the consent of the data subject. Under the circumstances we will disclose requested data. However, the HR Manager will ensure the request is legitimate, seeking assistance from the Data Manager and from the company's legal advisers when necessary.

Providing information.

We aim to ensure that individuals are aware that the data is being processed and that they understand:
How the data is being used.

How to exercise their rights.

To this end, the company has a privacy statement setting out our data relating to individuals issues by the company.

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