Data Protection Policy

Introduction

In order to carry out our services the Gunite Group must collect and use personal data and sensitive personal data relating to the people with whom and for whom we work. These can include customers, suppliers, business contacts, employees and other people the group has a relationship with or may need to contact.

This policy describes how this data must be collected, handled and stored to meet the company's data protection standards and comply with the law.

Policy Scope

This data protection policy applies to The Gunite Group and all employees, contractors, suppliers and other people working on behalf of the company to ensure that the company:

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

It applies to all data the company holds relating to identifiable individuals which can include:

- Names of individuals
- Postal address
- Email addresses
- Telephone numbers
- Any personal information relating to individuals

Data Protection Law

The Gunite Group will manage any personal data in accordance with the Data Protection Act 1998 and other related or forthcoming legislation, whether that information be on paper, databases, emails, CCTV, telephone records, or by any other means. We understand our obligations to ensure that personal data is managed fairly, lawfully, accurately and securely.

The Gunite Group will follow the eight principles of the Data Protection Act 1998, these principles require that all data shall be:

1. Processed fairly and lawfully
2. Be obtained for specific and lawful purposes
3. Adequate, relevant and not excessive
4. Accurate and up to date
5. Not be kept for longer than is necessary
6. Processed in accordance with the rights of data subjects
7. Processed securely and protected in appropriate ways
8. Not be transferred to a country or territory outside the European Economic Area without adequate safeguards

The Gunite Group will review data protection strategies on a regular basis and put in place any appropriate technical, training, organisation, administrative and security procedures that are necessary.

This policy and any revisions thereto will be made available to all current and new employees who are collectively and personally responsible for understanding this policy and the practical application thereof. The policy will also be available for any interested parties on request.

General Staff Guidelines

- The only people to access data covered by this policy are 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 Gunite Group will provide training to all those employees that handle personal data to help them understand their responsibilities.
- Employees should keep all data secure, by taking sensible precautions and following the guidelines in 'Data Storage' below.
- Strong passwords must be used and never shared.
- Data should be regularly reviewed and updated. If it is found to be out of date or no longer required it should be deleted and disposed of, unless there are legitimate legal or business reasons for keeping data for longer.
- If an employee is unsure about any aspect of Data Protection they should ask their line manager.

Data Storage

- When data is stored on paper, it should be kept in a secure place where unauthorised people cannot access it.
- When data usually stored electrotonically is printed out for some reason it must be kept in a locked drawer or filing cabinet.
- Once paper documents are finished with they must be shredded, and we provide such central facilities for this to happen .
- Electronic data must be protected from unauthorised access, accidental deletion and malicious hacking attempts.
- Electronic data should be backed-up regularly in line with the company's backup IT procedures
- All servers and computers containing data should be protected by approved security software and a firewall.
- Data stored on a computer should be protected by strong passwords that are changed regularly.
- Servers containing personal data must be kept in a secure location, away from general office access.
- Data stored on CDs or memory sticks must be locked away securely when they are not being used.
- Data should never be saved directly to mobile devices such as laptops, tablets or smartphones unless the same rules on the security of data are applied.

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

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

Data retention

We must retain personal data for no longer than is necessary. What is necessary will depend on the circumstances of each case, taking into account the reasons that the personal data was obtained, but should be determined in a manner consistent with our data retention guidelines.

Data Protection Breaches

It should be noted that ignorance does not normally amount to a reasonable defence and disciplinary action may be taken if any of the following breaches occur.

- Browsing your own computer or paper records without appropriate authorisation and a legitimate business reason
- Browsing computer or paper records of friends, colleagues or customers without appropriate authorisation and a legitimate business reason
- Data lost or compromised
- Using customer or employee personal data or information without appropriate authorisation and a legitimate business reason
- Disclosing customer or employee personal data or information without appropriate authorisation and a legitimate business reason
- Disclosing computer passwords
- Any other breach of personal data protection

Reporting breaches

All members of staff have an obligation to report actual or potential data protection compliance failures. This allows us to:

- Investigate the failure and take remedial steps if necessary
- Maintain a register of compliance failures
- Notify the relevant authorities of any compliance failures that are material either in their own right or as part of a pattern of failures

Subject access requests

Individuals are entitled, subject to certain exceptions, to request access to information held about them.

If you receive a subject access request, you should refer that request immediately to<insert your chosen job title>. We may ask for your full co-operation to help us comply with those requests.

Please contact the HR Department if you would like to correct or request information that we hold about you. There are also restrictions on the information to which you are entitled under applicable law.

Training

Staff will receive training on the use, storage and disposal of data relevant to their job role especially if they have access to personal sensitive data . New joiners will receive relevant data training as part of their induction process. Further in-house training may be provided as part of a periodic refresher process or whenever there is a substantial change in the law or our policy and procedure.