

# SIG Data Protection Policy



## **Introduction**

SIG plc is fully committed to compliance with the requirements of the UK's Data Protection Act 1998 and the Republic of Ireland's Data Protection Acts 1988 and 2003. SIG UK and Ireland based businesses will therefore follow procedures that aim to ensure that all employees, contractors, agents, consultants or other servants of SIG plc who have access to any personal data held by or on behalf of SIG plc, are fully aware of and abide by their duties and responsibilities under the Data Protection Acts.

## **Statement of Policy**

In order to operate efficiently, SIG plc has to collect and use personal data about people with whom it works. These may include members of the public, current, past and prospective employees, clients, customers, and suppliers. This personal information must be handled and dealt with properly, regardless of how it is collected, recorded and used, and whether it be on paper, in computer records or recorded by any other means, and there are safeguards within the Acts to ensure this.

SIG plc regards the lawful and correct treatment of personal data as very important to its successful operations and to maintaining confidence between SIG and those with whom it carries out business. SIG plc will ensure that it treats personal data lawfully and correctly.

To this end SIG plc endorses and adheres to the Principles of Data Protection as set out in the UK's Data Protection Act 1998 and the Republic of Ireland's Data Protection Acts 1988 and 2003.

## **The Principles of Data Protection**

SIG UK and Ireland will abide by the Data Protection Principles for the UK and the Republic of Ireland.

The UK's Eight Data Protection Principles require that personal data is:

- Fairly and lawfully processed;
- Processed for limited purposes;
- Adequate, relevant and not excessive;
- Accurate and up to date;
- Not kept for longer than necessary;
- Processed in line with the individual's rights;
- Secure;
- Not transferred to other countries without adequate protection.

The Republic of Ireland's Eight Data Protection Principles require that personal data is:

- Obtained and processed fairly;
- Kept only for one or more specified and lawful purposes;
- Processed only in ways compatible with the purposes for which it was initially given;
- Kept safe and secure;
- Kept accurate and up-to-date;
- Adequate, relevant and not excessive;
- Retained no longer than is necessary for the specified purpose or purposes;
- Provided to any individual who requests a copy of their own personal data.

Any data processing which takes place within the Republic of Ireland will adhere to the Data Protection Acts of 1988 and 2003 and the Data Protection Commissioner whereas data processing within Northern Ireland will be governed by the Data Protection Act 1998 and the Information Commissioners Office.

## **Roles and Accountabilities**

### **All Managers**

In addition to the above, all Managers are responsible for ensuring their direct reports are aware of the employee's obligations under the Data Protection Acts, this policy and the Data Protection Procedure Manual, for the holding and processing of personal data.

## **All Employees**

Employees are responsible for:

- Checking that personal data provided in connection with their employment is accurate and up to date;
- Notifying SIG plc in writing if this data changes to ensure personal data provided is accurate and up to date, for example, change of address, name, etc.;
- Ensuring that any personal data, whether in electronic or paper format, is held and processed securely;
- Following the procedures within the Data Protection Procedure Manual.

## **Disclosure**

Personal data will not be disclosed to a third party without the consent of the individual, unless the disclosure is permitted by law under statute, is necessary for the prevention or detection of crime or will prevent injury or harm to the individual or their property. All disclosure requests will be dealt with by the Compliance Department and in accordance with the Data Protection Procedure Manual.

## **Notification to the Information Commissioner and the Data Protection Commissioner**

### **Information Commissioner**

The Information Commissioner (ICO) maintains a public register of data controllers within the United Kingdom. SIG plc and its subsidiary companies are registered as such. The Data Protection Act 1998 requires most data controllers that process personal data, to notify and renew their notification, on an annual basis.

To this end the Data Protection Officer will be responsible for notifying and updating the Information Commissioner of the processing of personal data, within the company. The Data Protection Officer will review the Data Protection Registration annually, prior to notification to the Information Commissioner. Any changes to the registration will be notified to the Information Commissioner, within 28 days.

### **Data Protection Commissioner**

The Data Protection Commissioner maintains a public register of data controllers within the Republic of Ireland. SIG plc and its subsidiary companies are not registered as such, as there is no legal obligation to do so given the level of data processing within SIG. The Data Protection Officer will notify the Data Protection Commissioner if the level of data processing within SIG changes to the point that notification is required.

## **Implementation**

SIG has appointed a Data Protection Officer (Mark Smith). This officer and senior management will be responsible for instigating the implementation of this policy throughout the company. The Data Protection Officer and senior management will ensure that:

- Sufficient data protection training is provided, for employees within SIG;
- Data Protection procedures are developed, implemented and maintained;
- Compliance checks are conducted to ensure adherence, throughout the company, with the procedures and applicable Data Protection Acts.

The Group Chief Executive has lead responsibility for policy implementation within the Group and this policy is signed by the CEO to demonstrate the Board's commitment. A copy of this policy is also posted on the SIG plc web site at [www.sigplc.com](http://www.sigplc.com).



Stuart Mitchell  
**Group Chief Executive**