



Corporate Governance

# Group General Data Protection Regulation (GDPR) Policy



## INTRODUCTION

In order to operate efficiently, we often collect and use data about people with whom we work. This can include data from our current, past or prospective employees, customers, clients, suppliers and the general public. This information is called 'personal data', and it must be handled, stored, managed and destroyed properly to ensure that we are compliant with the General Data Protection Regulation (GDPR) that governs data protection across the countries in which we operate.

This policy outlines what we expect from all employees in the collecting, handling and storing of personal data.

It applies to all employees across the Group. You should also refer to the relevant local policy, procedures and legislation for your country or area of business. As an employee, you should make sure that you are aware of your responsibilities and obligations when accessing, using, storing, transmitting or sharing personal data.

The policy also applies to contractors, agents, consultants or any others working for or on behalf of SIG plc.

*In this document 'SIG' refers to SIG plc and its affiliate companies. 'Our' and 'we' refers to SIG plc.*

## PRINCIPLES OF GDPR

Personal data is anything that can identify an individual and can include information such as a name, a photo, an email address (including work email address), bank details, medical information or even a computer IP address when combined with other information or when used to build a profile of an individual, even if that individual's name is unknown.

We are committed to managing any personal data in the correct way by ensuring that it is managed and processed according to the principles below:

- **Lawful, fair and transparent:**  
We will comply with GDPR regulations and do what we say we are going to do with any data that is collected, in a specific period of time. Being transparent means that we will allow data subjects (for example, employees or customers) to know what data we are holding on them and knowing when they can opt out of their data being collected or stored. You must ensure that you process personal data lawfully, fairly and in a transparent manner in relation to the data subject.
- **Purpose limitation**  
We will only use and keep data for the stated purpose, that the data subject has agreed to. You must only collect personal data for a specific, explicit and legitimate purpose, clearly stating what the purpose is and only collecting data for as long as necessary to complete that purpose.
- **Data minimisation**

We will only collect sufficient data to achieve the intended purpose and will not collect or store more data than is necessary. You must ensure that personal data you process is adequate, relevant and limited to what is necessary in relation to your processing purpose.

- **Accuracy**

We will ensure that any data that is stored is accurate and is fit for purpose. Data subjects have the right to update or correct their data and we will ensure that the correct subject access management is in place to allow this. You must take every reasonable step to update or remove data that is inaccurate or incomplete. Individuals have the right to request that you erase or rectify inaccurate data that relates to them, and you must do so within a month of being notified.

- **Storage limitation**

We will delete any data once it is no longer needed to fulfil its intended purpose. You must delete personal data when you no longer need it. The required timescales to delete data will depend on the circumstances and the reasons why you collect this data. Make sure that you do not have historical emails that may contain personal data. For further information on relevant timescales, please contact the Group General Counsel.

- **Integrity and Confidentiality**

We will ensure that data is kept confidential. We will perform risk assessments and ensure that appropriate security measures are taken for all data that is held. You must keep personal data safe and protected against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

- **Accountability**

We will comply with GDPR regulations in all areas of the business and ensure that we have the right systems, processes and measures in place. You must take responsibility for what you do with personal data and how you comply with the other principles. You must have appropriate measures and records in place to be able to demonstrate your compliance.

## RESPONSIBILITIES

To ensure that we are consistently applying policies and principles of data protection across the Group, we have an executive sponsor and dedicated individuals who drive the standards of compliance that we must adhere to. Alongside the data protection roles, senior management is responsible for ensuring that the standards expected are upheld, to ensure that sufficient data protection training is provided to employees, data protection procedures are developed, implemented and maintained compliance checks are conducted to ensure procedures and applicable legislation is adhered to throughout the Group.

### Employee responsibilities

As an employee, you are expected to understand any additional and applicable principles or laws in your country or area of business to ensure that you are compliant.

You should:

- ensure that any personal data, whether in electronic or paper format, is held and processed securely

- follow the principles in this policy and GDPR legislation and procedures to ensure that you are compliant

In addition, in relation to your own personal data, you should:

- check that personal data provided in connection with your employment is accurate and up to date
- notify your line manager or local HR representative if your data changes, for example, if you have a change of address or name. For areas where there is a HR system with self-service, you should make sure that you process any updates to your personal data through the correct system.

### **Management responsibilities**

If you are a manager, you should drive and ensure compliance with this policy in your teams. You are responsible for ensuring that your direct reports and their teams understand the expectations that are set out in the policy and that they are aware of their obligations under any relevant GDPR laws and processes in your area.

## **DISCLOSURE OF PERSONAL DATA**

You should under no circumstances disclose any personal data to a third party or another person internally or externally to the business without the consent from the individual the data refers to. The only exceptions to this would be where we were required to assist with legal proceedings, if it was necessary for the prevention or detection of any crime, or if the disclosure would prevent injury or harm to the individual or their property.

Where there is a legitimate interest for data to be processed by a third party this must be governed by a contract, agreement or other legal act.

In each country around the Group, there is a dedicated individual who is responsible for managing data protection. This responsibility may be the individual's full time role or may be a part of their role. If you receive a request to disclose personal data you should inform your line manager and the person who manages data protection before sending any information. It is important to note that data protection procedures may vary from country to country and local laws may take precedent. Therefore, please ensure that you are aware of the local legislation that may apply. If unsure, please see the person dedicated to managing data protection in your area.

## **FURTHER GUIDANCE AND SUPPORT**

If you have any questions on the content of this policy, or need further guidance or support, please contact your data protection representative or your local HR representative.

You can also find further information in the following related documents:

- Group Information Handling Policy (IT policy)

**Steve Francis**  
**Chief Executive Officer**  
Issue number: 02  
Date: March 2020  
Policy owner: Group General Counsel