## Policy Statement

As part of our commitment to ethical business, Morgan Sindall Group plc and its subsidiaries (hereinafter the 'Group' 'we' 'our') is committed to conducting our business with the highest standards of integrity and honesty; and in an open and ethical way. This includes compliance with all Data Protection laws and regulations.

The Group recognises that everyone has rights with regard to how their Personal Data is handled. During the course of our business we will collect, store and process Personal Data about our Employees, customers, suppliers and Third Parties and we understand the need to treat that information in an appropriate and lawful manner. The Group will keep Personal Data secure and only use it for the purposes for which it was obtained. In other words, we will treat all such information very carefully.

This policy sets out how we will handle the Personal Data which we collect or which is shared with us, and provides guidance for Employees about how to do the same.

A glossary of terms used throughout this Data Protection Policy can be found at the end of this document.

## What is Personal Data?

Personal Data includes data in our possession related to any living individual and which can be used, either directly or in conjunction with other data, to identify that individual. Personal Data can be factual (such as a name, address or date of birth) or it can be subjective (such as an opinion about that person, their actions and behaviour).

## Data Protection Principles

The Group needs to keep certain information about its Employees, customers and suppliers for financial and commercial reasons, such as to pay salaries to staff, keep records of training and for health and safety purposes.

Personal Data must be:

1. processed fairly, lawfully and transparently and, in particular, not be processed unless certain conditions are met. To do this, Personal Data must only be processed for one of a very few reasons. These include, amongst other things, only processing data where we have the Data Subject's Consent to the processing or the processing is necessary for the performance of a contract with the Data Subject – such as an employment contract.
   Sensitive Personal Data is a special category that must be handled with extra care. This data may only be processed with the Explicit Consent of the Data Subject.

2. collected for specified, explicit and legitimate purposes, and the Data Controller shall limit the processing of that Personal Data to only what is necessary to meet the specified purpose or purposes.

3. adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

4. accurate and, where necessary, kept up to date

5. not be kept for longer than is necessary for the purpose or purposes for which it was collected.

6. processed in accordance with the rights of Data Subject. The Data Subject has rights:-
   - of access to a copy of the information comprised in their Personal Data;
   - to object to processing that is likely to cause or is causing damage or distress;
   - to prevent processing for direct marketing;
   - to object to decisions being taken by Automated Means;
   - in certain circumstances to have inaccurate Personal Data rectified, blocked, erased or destroyed; and
   - to claim compensation for damages caused by a breach of the General Data Protection Regulation ((EU) 2016/679) (GDPR).

7. processed in a manner that ensures appropriate security of the Personal Data to ward against unauthorised or unlawful processing, accidental loss, destruction of, or damage to, Personal Data.

8. Personal Data shall not be transferred to a Third Country or an international organisation unless we have ensured an adequate level of protection for the rights and freedoms of Data Subjects in relation to the processing of Personal Data.

Further detailed information on the Data Protection Act 1998, the GDPR and Personal Data, beyond the principles laid out above, can be found by visiting the website of the Information Commissioner's Office www.ico.org.uk .

**Data Processing**

Where we undertake data processing activities we will implement appropriate technical and organisational measures to ensure the protection of the Data Subject's rights. These measures include the use of encrypted laptops and removable media. Any processing we undertake will be with the Consent of the Data Subject, or will be governed by a contract.

Where processing is undertaken by third parties on our behalf, such as the administration of the pension scheme, there will be a contract in place which complies with the GDPR, and dictates the terms upon which processing is allowed. Personal Data is only processed on our instructions and is kept confidential. All processing will comply with Article 32 of the GDPR.

**Data Protection Impact Assessments**

Any new or significant change to our processes, procedures or systems must be assessed for impacts on the holding, Processing or protection of Personal Data. A two-stage guide has been developed by the MS Information Security team, to consider whether there is an impact, and if so what will be required. Any such proposed changes should be referred by the business sponsor concerned to infosec@morgansindall.com as soon as possible, and they will assist with the assessment process.

**Data Security**

The Group will process the data we hold in accordance with all applicable Group Policies. These policies require us to operate a range of controls to secure personal information against unlawful or unauthorised Processing and against the accidental loss of, or damage to, Personal Data.

### Data Subject Access Requests

Data Subjects can make a request for information we hold about them. All Data Subject access requests should be sent to infosec@morgansindall.com and the information security team will respond.

### Responsibilities

All Employees are responsible for ensuring that Personal Data held, processed or used, on behalf of or by the Group, is handled in accordance with the above principles; is not disclosed to anyone not authorised to receive it; and is used only for the purposes for which it was obtained.

### Data Breach response

If a Breach of Personal Data is suspected, the incident should be notified via e-mail to GDPR@morgansindall.com as soon as possible.

### Enforcement

Any Employee found to have deliberately violated this policy may be subject to disciplinary action up to and including dismissal, in line with current divisional Human Resources policies.

In the event that Group and Divisional policies are conflicting, Group Policy is overriding.

If you have any questions about this policy or need further assistance on Data Protection matters, please ask the Group General Counsel or the Information Security Team on GDPR@morgansindall.com.

**GLOSSARY OF TERMS**

| | |
|---|---|
| Automated Means | Decisions taken by such means require no human involvement or interpretation, other than data input, and include credit-scoring or Profiling. |
| Consent | Any freely given, specific, informed and unambiguous indication of the Data Subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the Processing of Personal Data relating to him or her. |
| Data Breach | A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed. |
| Data Controller | A Natural or legal Person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data. |
| Data Processors | A Natural or Legal Person, public authority, agency or other body which Processes Personal Data on behalf of a Data Controller. |
| Data Protection | The process of safeguarding Personal Data from unauthorised or unlawful disclosure, access, alteration, Processing, transfer or destruction. |
| Data Protection Officer | The accountable person within the organisation responsible for the protection of Personal Data. |
| Data Subject | The identified or Identifiable Natural Person to which the data refers. |
| Employee | An individual who works part-time or full-time for the Group under a contract of employment, whether oral or written, express or implied, and has recognised rights and duties. This includes temporary employees and independent contractors. |
| Encryption | The process of converting information or data into code, to prevent unauthorised access. |
| Explicit Consent | Consent expressly confirmed in words, preferably in writing, evidenced and retained. |
| Identifiable Natural Person | Anyone who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that Natural person. |
| Information Commissioner's Office (ICO) | An independent Public Authority responsible for monitoring the application of the relevant Data Protection regulation set forth in national law. (www.ico.org.uk) |
| Office of Data Protection | The team within Morgan Sindall Group which undertake the responsibilities of the Data Protection Officer. |
| Personal Data | Any information (including opinions and intentions) which relates to an identified or Identifiable Natural Person. |
| Process, Processed, Processing | Any operation or set of operations performed on Personal Data or on sets of Personal Data, whether or not by Automated Means. Operations performed may include collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. |
| Profiling | Any form of automated processing of Personal Data where it is used to evaluate specific or general characteristics relating to an Identifiable |

| | |
|---|---|
| | Natural Person. In particular to analyse or predict certain aspects concerning that Natural Person's performance at work, economic situations, health, personal preferences, interests, reliability, behaviour, location or movement. |
| Sensitive Personal Data | Data pertaining to or revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership; data concerning health or sex life and sexual orientation; genetic data or biometric data. |
| Third Country | Any country not recognised as having an adequate level of legal protection for the rights and freedoms of Data Subjects in relation to the Processing of Personal Data. |
| Third Party | An external organisation with which the Group conducts business and which is also authorised to, under the direct authority of the Group, Process Personal Data of Employees or Contacts. |

**Revision schedule**

| Rev No | Date of issue | Next Revision Date | Details of Change | Owner |
|---|---|---|---|---|
| 1.0 | 1st Jan 2015 | 1st Jan 2016 | Created by Chris Russell-Miller | Head of Information Security & Compliance |
| 1.1 | 1st March 2016 | 1st March 2017 | Annual Review | Head of Information Security & Compliance |
| 1.2 | 1st April 2017 | 31st March 2018 | Annual Review | Head of Information Security & Compliance |
| 1.3 | 1st April 2018 | 31st March 2019 | Annual Review & Update to reflect introduction of GDPR | Head of Information Security & Compliance |
| 1.4 | 12th July 2018 | 31st July 2020 | ISO27001 Review | Head of Information Security & Compliance |
| 1.5 | 13th July 2018 | 31st July 2020 | Approved for publication | Group General Council |
| 1.6 | 18th November 2020 | | Rebranding | PA to IT Director |