MORGAN SINDALL GROUP

Data Protection and You

Morgan Sindall Group Data Protection Policy

Version 2.1 · 28th Mar 2023

John Morgan,
Chief Executive

A message from John

In order to manage our business effectively and to meet the expectations of our customers and other stakeholders, all of the companies within our Group collect and process Personal Data. We maintain the highest standards of honesty and integrity across the Group which means that we respect the right to privacy of all individuals, and we understand our obligation to protect all of the Personal Data that is collected by Group or shared with us.

The unauthorised use or disclosure of Personal Data can cause harm to individuals, undermine trust and damage our reputation. For this reason, we all have a part to play in safeguarding the privacy of the personal data of our colleagues, business partners and customers.

This policy will help you to understand your rights and responsibilities with regard to the handling of Personal Data. If you are unsure about any aspect of the Policy or have questions, please speak to your line manager or the Information Security & Compliance team - dataprotection@morgansindall.com

We all have an important role to play as we build new infrastructure, create better workplaces, and regenerate cities – with openness, honesty and integrity.

MORGAN SINDALL GROUP

When we are entrusted with anyone's Personal Data, we will protect it from misuse.

Our Data Protection policy applies to:

Who?

- Everyone who works for us whether they are permanent, contract and temporary employees;
- Contractors, agency workers and colleagues working in joint venture with us;
- Employees of third parties engaged by the Group.

What?

- Personal Data related to any living person and which can be used to identify that individual.

Where?

- All Group, third party or supplier's facilities
- Any location where one of our devices or systems to process Personal Data, including home offices, is used.

Just to remind you when we say personal data we mean things like your:
name, address, phone number, email addresses or sexual orientation, any disabilities, ethnicity, religion, trade union membership

If you are unsure if something is personal data or not, please contact the Information Security & Compliance Team, the Group General Counsel or your business Head of Legal.

What Personal Data do we process?

In order to manage our business, we need to collect, store and process Personal Data about our employees as well as individuals employed by our customers, suppliers and other third parties.

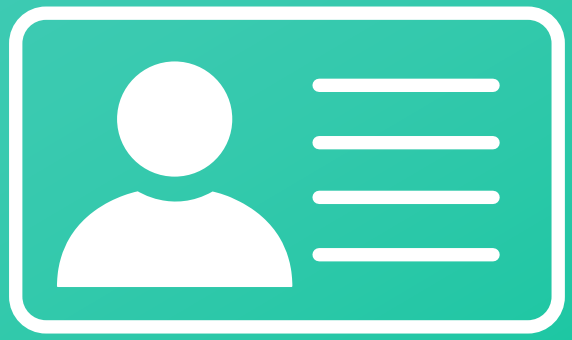
We need to process Personal Data for financial and commercial reasons, such as to pay salaries, keep records of training and for health and safety purposes. We understand the need to treat any Personal Data we collect or that is shared with us in an appropriate and lawful manner.

We also process some types of Personal Data that are likely to be more sensitive and require extra protection. Examples include:

- Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership;
- Genetic or biometric data, such as a fingerprint;
- Data concerning health, a person's sex life or sexual orientation.

Rights and responsibilities

The law affords rights to individuals with respect to their Personal Data and places obligations and responsibilities on us when we are collecting, processing or storing it.



Everyone has the right to:

- access a copy of their Personal Data;
- object to processing of their Personal Data that is likely to cause or is causing damage or distress;
- prevent their Personal Data, being processed for direct marketing purposes;
- object to decisions being taken by automated means;
- have inaccurate Personal Data rectified, blocked, erased or destroyed;
- claim compensation for damages caused by a breach of the Data Protection Act 2018.

It's important that we respond to any requests from Data Subjects to access their Personal Data in a timely and efficient manner.
All such requests should be passed immediately to the information security team on:
dataprotection@morgansindall.com

It's just as important that we respond to any requests from Data Subjects to change or delete their Personal Data, but these changes are to be dealt with at divisional level and you should seek guidance from your business IT team.

We have a responsibility to:

- process Personal Data fairly, lawfully and transparently;
- collect Personal Data for specified, explicit and legitimate purposes;
- collect Personal Data that is adequate, relevant and not excessive for the specified purpose;
- limit the processing of Personal Data to only what is necessary to meet specified purposes;
- ensure that Personal Data is accurate and, where necessary, kept up to date and not kept for longer than necessary;
- keep Personal Data secure and protected from unauthorised or unlawful processing, accidental loss, destruction or damage;
- prevent the transfer of Personal Data 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.

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, or the processing is necessary for the performance of a contract with the Data Subject – such as an employment contract.

Data security

We have in place a range of controls to protect Personal Data against both unlawful or unauthorised processing and accidental loss or damage. If something does go wrong and you suspect there has been a potential or actual breach of Personal Data, it's vital that you let us know as soon as possible to enable us to act quickly. You should immediately inform dataprotection@morgansindall.com

And finally...

This policy document sets out our rules and best practices, however if you are in doubt about anything or if you have a question about how to protect Personal Data, please contact the Information Security & Compliance Team, the Group General Counsel or your business Head of Legal.

Alternatively, visit the Information Security & Compliance SharePoint site ("The Vault") which contains lots of useful information on IT and data privacy. You can also refer to the Data Protection Policy (DPP) Extended Guidance (EG) which is available on the Group SharePoint site ("Pulse").

And now for the small print:

Responsibilities: All users of IT systems which are used for collecting, storing or otherwise processing Personal Data delivered by or on behalf of Group are responsible for ensuring compliance with this policy.

Conflict: In the event that Group and Divisional policy are conflicting, this policy is overriding.

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.

Monitoring: We reserve the right to monitor any and all use of the computer network. To ensure compliance with Group policies this may include the interception and review of any emails, internet usage logs, instant message logs or other messages sent or received, or inspection of data stored on personal file directories, hard disks, and removable media.

MORGAN SINDALL GROUP

Raising Concerns

As part of our commitment to ethical business, we are 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 relevant data protection laws and regulations including the UK General Data Protection Regulation in the countries where the Group operates.

If you see anything that you believe does not uphold these standards, then please tell us. We will listen, we will take your concern seriously, we will investigate it thoroughly and we will maintain confidentiality.

Speaking up about wrongdoing at work is always the right thing to do. It can be hard, but we will protect you from any form of retaliation. Raising concerns in good faith will never disadvantage your career.

You can raise a concern with your line manager or by making a call to Raising Concerns – the Group's whistleblowing hotline. All calls are taken by Safecall, an independent organisation with specially trained and impartial staff. The service is available 24 hours a day and 7 days a week. Safecall can be contacted on 0800 915 1571 or online at www.safecall.co.uk/report

Further information about raising concerns can be found in our Whistleblowing Policy and Procedure.