

Data Protection Policy

20 August 2021



Data Protection Policy

Application

This Policy applies to all Pellikaan Construction Ltd (Pellikaan) staff. It sets out our requirements and expectations in order for the company to meet applicable law.

Pellikaan aim to protect the confidentiality and integrity of personal data. This is a critical business responsibility. All of our staff are required to operate in accordance with the Policy and apply it in the workplace.

We comply fully with the Data Protection Act 2018 and UK General Data Protection Regulation (UK GDPR).

Personal Data

Personal data is data relating to a living individual who can be identified from that data (or when combined with other data held). Personal data can be factual (e.g., name, employee number, date of birth) or it can be a view or opinion about that person, their actions and behaviour.

In accordance with the Data Protection Act 2018 and UK GDPR, we shall ensure that personal data shall be:

- Processed fairly, lawfully, and transparently.
- Obtained only for specified and legitimate purposes and shall not be processed in any manner which is incompatible with those purposes.
- Adequate, relevant, and not excessive with respect to the purposes for which it is processed.
- Accurate and, where appropriate, kept up to date.
- Kept for no longer than is necessary in respect of the purpose(s) for which it is processed.
- Processed in accordance with the rights of data subjects. (A data subject is a living individual).
- Protected against unauthorised or unlawful processing, accidental loss, destruction, or damage through appropriate technical and organisational measures.
- Made available to data subjects, who are allowed to exercise certain rights in respect of their personal data.

These principles lie at the heart of our approach to the processing of personal data.

Policy approach

Pellikaan is committed to complying with all aspects of data protection legislation in its handling of personal information. This information relates to customers, suppliers, and staff.

We will ensure that:

- We aim to build trust with our clients, treating them as we, ourselves, would wish to be treated and in line with what they would reasonably expect. We aim to avoid unjustifiable or adverse effects in processing data.
- Data is held securely. In order to prevent unauthorised access or disclosure, we have put in place reasonable physical, electronic, and managerial procedures to safeguard data collected. (Procedures are detailed below).
- Personal data is stored only for pre-identified processing purposes (i.e., for what we need) or on statutory grounds. We ensure that it is not stored for any longer than necessary. Data is deleted in a timely manner and any hardcopy data is securely shredded.

- Paper-based data is treated with the same duty of care as electronic.
- We ensure that paper-based data is held securely in locked filing cabinets when not in use.
- Our staff operate a clear desk policy when away from their desks.

Comprehensive IT data security procedures are in place:

- Pellikaan carries Cyber Essentials certification under Certificate Number IASME-CE-012594.
- It is our standard working practice for staff to lock their PC when away from the desk.
- All computers – whether desk, laptop or tablet are password protected and encrypted.
- Tablet computers and laptops used by our field-based staff are encrypted and have dual-level authentication requirements (password and via access code generated by an App on mobile device).
- All passwords have to be alpha-numeric and contain one of a series of special characters. They are, therefore, considered very strong.
- Staff are not allowed to share their password or access code with any third party.
- Our email system and digital files are hosted securely, with the protection of an industry standard firewall and virus, intrusion, and malware software.
- Data is stored securely within the EU on firewalled and virus, intrusion and malware protected servers and our technology platform complies fully with UK GDPR requirements.
- Staff are allowed access only to systems and data required to carry out their jobs efficiently and effectively.

Access to and maintenance of data

We are committed to allowing individuals appropriate access to information held about them and to a regular process of updating and/ or secure deletion/ destruction of out-of-date information.

In accordance with the Data Protection Act 2018 and UK GDPR, Pellikaan is committed to ensuring all data subjects have the right to:

- Be informed about how their personal data is processed.
- Request access to any personal data held about them.
- Request inaccurate personal data to be rectified or incomplete information to be completed.
- Request erasure of personal data in certain circumstances.
- Restrict processing of personal data in certain circumstances – e.g., that held for any direct marketing purpose.
- Data portability – the transfer of personal information to another organisation, or to the data subject, in certain circumstances.
- Object to the processing of their personal data in certain circumstances.

Rights in respect of automated decision making are not applicable in our business, as we do not carry out these practices.

These rights are reflected in our publically available Privacy Statement.

Data sharing

Personal data may be shared externally if there is a legal basis to do so (e.g., in connection with a contract; legal obligation; legitimate interest).

Personal data may also be disclosed to third parties should Pellikaan buy or sell any business or assets, or if assets are acquired by a third party.

Data sharing protocols

The following protocols will be applied:

- Clarity surrounding precise data to be shared, whether this actually needs to be shared and with whom.
- Risks to the data subject will be assessed and mitigated prior to sharing data.
- Minimisation of data shared, so that it reflects only the data that is required.
- Consideration of whether the objective in sharing data can be achieved if that data is anonymised.
- Secure handling of data, through a suitable mode of sharing.
- Recipients of data will be limited to those who 'need to know'.
- Frequency of data sharing will be limited to that which is absolutely necessary.
- Data transferred outside of the EU (where processed) will meet EU & UK GDPR rules, with appropriate safeguards in place. Data transfer must be approved at top level within our business.

Staff data

We ensure our staff are aware of their own personal data which we maintain on file, and the rationale for this. Pellikaan will request their permission/ removal instructions in respect of continued maintenance, ensuring these are observed.

Culture & training

We will build and maintain a culture of data responsibility.

Pellikaan will do this by:

- Running internal awareness campaigns (already started) - through office-based posters and a video presentation - accessible easily and at any time via the Pellikaan intranet. These campaigns focus on compliance, risks, and risk management strategies.
- Training our staff in the application of the Data Protection Act & UK GDPR in the workplace and in how to comply with the eight rights that individuals have concerning their data, with regular refresher training taking place.
- Making attendance at training sessions mandatory for Directors, Managers, Supervisors, and wider staff.
- Ensuring that all our customer-facing staff – e.g., Directors, Project Managers, Site Managers are aware of our procedures and working practices and their responsibilities under the Data Protection Act and UK GDPR.
- Embedding our Data Protection Policy and Privacy Notice within the Pellikaan Employee Management System.

Dealing with data breaches

Pellikaan has a data breach protocol in place, and our staff are trained fully in its implementation.

Examples of data breaches (not listed comprehensively) are:

- Unauthorised deletion of personal data.
- Transmission of data to an unintended party.
- Data leakage from a laptop or mobile device.
- Amendment, misplacement, or alteration of personal data without permission.
- Data lost through cyber attack
- Unauthorised access to data.

Prompt action will be taken should a data breach occur, as time is of the essence. In such cases we will carry out: Identification of breach; Assembly of our Incident Response Team; Communication with all relevant parties; Securing of all systems; Evaluation and implementation of lessons learned. Pellikaan will report any notifiable breach to the Information Commissioners Office without undue delay.

Privacy Notice

Pellikaan has a UK GDPR compliant Privacy Statement in place, which is available publically through its website.

It confirms that Pellikaan Construction Ltd is the Data Controller.

The Privacy Statement covers:

- The basis for processing personal data.
- Methods of collecting personal data.
- Information security protocols.
- Rights of the data subject.
- Who to contact regarding those rights.
- How to file a complaint or request further information.

A copy of the Privacy Statement can be found below.



Privacy-Statement-1
81102.pdf

Responsibility and Authorisation

Our Managing Director provides top level commitment to data protection and has signed this Policy as such.

He is supported in doing so by Anton de Jongh, HR Manager at Pellikaan – who takes the lead on GDPR, and data protection matters.

Signed:

A handwritten signature in blue ink, appearing to read 'Gert-Jan Peeters', written over a horizontal line.

Name: Gert-Jan Peeters

Designation: Managing Director

Date: 20 August 2021

