



Data Privacy Statement

Frontier Pitts is the British Manufacturer of HVM & Security Gates, Barriers, Blockers, Bollards & Turnstiles. We are delighted that you have shown interest in our products and services. The following policy includes the importance of data security and data protection.

1. Personal Data

Information which is used in order to be able to draw conclusions about you, in other words personal or factual circumstances, must comply to the EU's GDPR Regulation. General Data Protection Regulation (GDPR) impacts how businesses collect and process data from individuals who live in the European Union (EU). This replaces the 1995 Data Protection Act.

2. Data Collection and processing

2.1 Frontier Pitts Ltd collects and processes information to be able to provide you with information in the future. Personal evaluation of your data does not take place.

2.3 Frontier Pitts ensures that anonymity is maintained pursuant to data protection.

3. Use and Forwarding of Personal Data

3.1 All of your personal data prepared for creation of your user account is treated as confidential by us and is not forwarded to third parties without your consent.

4. Use of Cookies

4.1 The website uses "cookies", text files which are stored on your hard drive. This text file contains information about your visit on our website. Other websites cannot look at or process this stored data.

4.2 You may prevent installation of cookies via appropriate setting of your browser software. However, we point out to you that in this case you may possibly be unable to use all functions of this website in their entirety.

5 Consent

Frontier Pitts will log your consent concerning data collection and storage. We will inform you when and how you have given your consent on request.

6 Data Security

6.1 Frontier Pitts utilise extensive technical and organisational security measures to protect your personal data from deliberate manipulations, loss, or access by unauthorised third parties. These measures are constantly improved within the scope of applicable data protection laws and in accordance with technological developments. These measures

include Anti-Virus Software, fire walls and passwords protection. Please also see out IT Security Policy at the end of this document.

7 Changes

We reserve the right to change the data privacy statement at any time with due regard to applicable data protection regulations.

8 Contact & Right to Information

Please contact us for further questions or suggestions concerning the data protection topic. In addition, you may obtain information at any time about the data stored by us concerning you. On request, please write to:

Marketing of Frontier Pitts Ltd. Crompton House, Crompton Way, Manor Royal Industrial Estate, Crawley, RH10 9QZ. Email: sales@frontierpitts.com

9 Right of Objection

Furthermore, you may revoke your consent for collection and storage of your personal data by Frontier Pitts at any time. On request, please write to the above-mentioned address or send an email.

IT Security Policy

Information Security Procedures for Restricted information and Higher.

All Frontier Pitts personnel on appointment are required to sign a Confidentially Agreement and actively follow the Information Security Procedure, which is audited by Frontier Pitts IT Department. The Project Manager will assign security roles and co-ordinate/review the implementation of information security, whilst ensuring that this is maintained over the period of the contract.

Frontier Pitts understands the importance of HR Security. All high-level personnel are screened, and references clarified. The roles and responsibilities of employees are defined and documented, with training received on information security awareness. Personnel who have committed a breach in security shall receive disciplinary action.

Frontier Pitts have a responsibility of asset for all client information. All protected information (whether held documents, received, or recorded, etc) and marked restricted or higher must be kept securely when not in use. Key holders allocated per project.

Processing of information will only be on a standalone system that has been approved for use with commercially marked documents. Commercially marked documents must not be transmitted across the company network, the internet, or any other network.

Any electronic storage will have detailed encryption and password only access.

Frontier Pitts personnel follow a clear desk, clear screen work policy when working with high security level projects. All personnel are instructed to log out of the computer system when away from the workspace.

Physical security measures such as physical safes, doors with secure locking devices and perimeter security such as gates and barriers shall be used to protect areas that contain information and information processing facilities

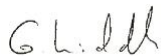
Internal personal clearance and formal vetting procedures to be followed – identification of documents must be clear, dated and number of copies recorded.

Loss or compromise of documents must be reported to the originator. Reproduction should not be carried out unnecessarily, without approval.

When travelling, carrying of this information should be locked in a briefcase and must not leave your possession except under exceptional circumstances. If travelling by car, sensitive information should be locked in the boot of the car at the start of the journey.

Destruction and disposal of information must be shredded at source.

Note: When working with high security level organizations such as the MOD, Nuclear, Government or HM Service companies, individual security guidance policies must be taken into consideration.



G Liddle

Frontier Pitts Ltd

January 2021