Customer Privacy Notice

1 Hermitage Innovation Group: Legal Entities

Hermitage Group Ltd – CRN 08355093

Border Merchant Systems Ltd – CRN 02542536

Fidelity Systems Ltd – CRN 03217771

Stratus21 Ltd – CRN 10089780

CIS Systems Ltd – CRN 08365507

2 Commitment to Information Security

We are providing you with this Privacy Notice in demonstration of our commitment to information security. We are registered with the Information Commissioner's Office under the following reference numbers:

Hermitage Group Ltd – ZA246246

Border Merchant Systems Ltd – ZA246233

Fidelity Systems Ltd – CRN 03217771

Stratus21 Ltd – ZA246239

CIS Systems Ltd – ZA246236

3 Information Security Management System (ISMS)

HIG Group operates and maintains an **Information Security Management System** (ISMS) in order to control its information assets and the information assets of its customers correctly. The ISMS is part of our '**privacy by design**' approach to data management and consists of the following components:

3.1 Contractual Agreements

HIG Group issues the following contractual documentation, which incorporate binding information security clauses, to employees, contactors, customers and suppliers:

	Employees	Contractors	Customers	Suppliers
Privacy Notice or Statement of Compliance for GDPR	√	√	√	√
Contract of Employment with Non Disclosure content	√			
Service Contract (or equivalent) with Non Disclosure content		√		
Commercial Terms of Business			√	

3.2 Policies & Protocols

HIG Group maintains operating policies and protocols to cover:

- Confidentiality
- Monitoring of communications
- Data breach reporting

HIG Group's relevant policies and protocols help us to fully realise our commitment to **lawful, fair and transparent** data processing.

3.3 Guidelines & Training

HIG Group commits to oversee the competence of all our human resources in respect of compliance with GDPR. This includes the issue of contractual and procedural documentation, as described above, as well as the implementation of training for all relevant members of staff.

Training is provided either directly by HIG Group or by their suppliers to enable employees and contractors to operate consistently within our ISMS.

3.4 Risk Assessment

HIG Group has run a GDPR audit to determine that our physical office environment, our IT systems, our personnel, our policies and our practices conform to the standards of the General Data Protection Regulation.

We are registered with the Information Commissioner's Office and we operate a formal incident management process to identify, contain and recover from a data breach, should one occur. Our employees are trained to report any suspicion of data breach to our Data Protection Officer in line with our Data Protection Policy.

4 Your Personal Information

4.1 Why we process your personal information

In the course of transacting with us you may be required to provide personal information to include: your name, address, telephone number, email address, and any feedback you give to us, including by phone, email, post, or when you communicate with us via social media.

Your personal information may be used by us to:

- Make our services and products available to you;
- Process your orders;
- Help us ensure that our customers are genuine and to prevent fraud;
- Find ways to improve our services and products;
- Contact you about services and products and services from us;
- Help answer your questions and solve any issues you have.

4.2 Your rights

4.2.i Access and correction

You have the right to access the personal information that we hold about you in many circumstances. This is sometimes called a 'Subject Access Request'. If we agree that we are obliged to provide personal information to you (or someone else on your behalf), we will provide it to you or them free of charge.

Before providing personal information to you or another person on your behalf, we may ask for proof of identity and sufficient information about your interactions with us that we can locate your personal information.

If any of the personal information we hold about you is inaccurate or out of date, you may ask us to correct it. If you would like to exercise these rights, please contact our Data Protection Representative, Dean Macken, dean@hig.limited

4.2.ii Right to stop or limit our processing of your data

You have the right to object to us processing your personal information if we are not entitled to use it any more, to have your information deleted if we are keeping it too long or have its processing restricted in certain circumstances. If you would like to exercise this right, please contact our Data Protection Representative, as detailed above.

4.2.iii How long will we keep your information?

We will retain a record of your personal information only for as long as it is necessary to do so. Our objective is to provide you with a high quality and consistent service across our group. We will always retain your personal information in accordance with law and regulation.

5 Our Suppliers & Third Parties

Qualifying the compliance of suppliers and third parties is essential to establishing our own Statement of Compliance with GDPR. Should any suppliers or third parties with whom we share personal information – either as data controllers or data processors – fail to evidence conformity to the requirements of GDPR (or fail to ameliorate their non-conformity under notice) we will terminate our relationship with them.

Our current key suppliers/third party in the context of personal information data processing have documented evidence of their compliance with GDPR.

6 Physical Security

HIG Group commits to protecting data through appropriate physical measures, these can be broken down into;

6.1 Premises Access Control

Access to all our office environments is physically controlled during business hours of 8.00 am to 5.30pm. Our premises are alarmed and a list of keyholders held at all times.

6.2 Server Access Control (Physical)

Server, routers and other business critical equipment is stored securely within each premises.

6.3 Server Access Control (Digitial)

Remote access to servers is carefully managed and monitored with enhanced security protocols in place.