Statement of Compliance with GDPR

1 Hermitage Innovation Group

Hermitage Innovation Group is a limited company registered in England no. 08355093

2 Commitment to Information Security

As a business Hermitage Innovation Group takes data security and privacy extremely seriously - we process personal information on behalf of our customers, and we also control the personal information of our own workforce. We are providing you with this Statement of Compliance with GDPR to help you to fulfil your own duties as a data controller in respect of supplier due diligence.

Hermitage Innovation Group Ltd is registered with the Information Commissioner's Office under reference No. ZA246246.

3 Information Security Management System (ISMS)

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

3.1 Contractual Agreements

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

	Employees	Contractors	Customers	Suppliers
Non-Disclosure Agreement	√	√		√
Contract of Employment	√			
Service Contract (or equivalent)		√		
Service Specification Agreement			√	
Commercial Terms of Business			√	

3.2 Policies & Protocols

Hermitage Innovation Group declares its operating policies and protocols, as specific to information security, within the following issued documentation:

	Employees	Contractors
Company Handbook	√	
Telecoms, IT, Internet & Email	√	
Data Protection	√	√
Information Security Incident Report form	√	√

The above documents provide clarity in respect of:

- Confidentiality
- Clear desk and clear screen policy
- Monitoring of communications
- Remote working
- Data disposal
- Data breach reporting

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

3.3 Guidelines & Training

Hermitage Innovation 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 members of staff.

Hermitage Innovation Group documents step by step procedural guidelines for its account management tasks and activities.

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

3.4 Risk Assessment

Hermitage Innovation Group has run an **Impact Assessment** 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. This assessment has been extended to verify the GDPR conformity of our key suppliers too.

Our **Impact Assessment** has established a Data Asset Register, classifying the data that we hold, identifying where it is stored, and articulating where risks may lie and how we can mitigate these. The establishment of a Data Asset Register enables Hermitage Innovation Group to respond rapidly, if required, to data access requests.

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 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 are as below, and have documented evidence of their compliance with GDPR.

Supplier	Privacy Measures & Statements
InkHR Consultancy for all our HR resource including payroll and employee benefits.	https://www.theinkgroup.co.uk/media/Privacy-Policy-v3.pdf
Breathe HR Software for our HR services: cloud based, self-service direct to employees.	www.breathehr.com/hr-software/security-reliability/
Mercer Hole Accountancy and Tax services: physical access and shared Dropbox folders	https://www.mercerhole.co.uk/tax-plus-blog/privacy-policy
Access Accounting Accounting software: on hosted server	www.theaccessgroup.com/privacy-and-legal/
Atlassian Jira - Development software tool: cloud based, self serve direct to employees	https://www.atlassian.com/legal/privacy-policy
Finastra BACS IP Software	https://www.finastra.com/privacy-policy
Microsoft O365 Email client	https://privacy.microsoft.com/en-gb/privacystatement

5 Physical Security

Hermitage Innovation Group commits to protecting data through appropriate physical measures, these can be broken down into:

5.1 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.

5.2 Server Access Control (Physical)

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

5.3 Server Access Control (Digitial)

Hosted (Cloud) Server access is via secure (SSL) connection. Passwords confirm to our password policy. Access to data is further restricted by IP Address.

All other systems where personal data is held are accessed either by MFA or secure passwords protected by a digital password vault and password randomisation protocol.

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

5.4 Portable Media

All portable media use by Hermitage Innovation Group is subject to encryption and / or password control.

5.5 Document Shredding & Disposal

Hermitage Innovation Group engages the services of ShredPro Ltd for the safe on site shredding and disposal of confidential waste. Prior to the removal of confidential waste from Hermitage Innovation Group's premises any confidential documents are stored in a locked console only accessible by one of the Company Directors.

EN15713 – European Standard of Information Destruction
BS7858 – operatives and drivers security vetting
ISO 14001 – environmental management

6 Cyber Security

Hermitage Innovation Group has committed to the standards of CyberEssentials to ensure cyber security independently verified by experts. Certification is anticipated in Q3 2018.

Within this framework we operate a range of data protection measures include Data Loss Prevention and the use of Secure File Transfer Protocols.