Privacy Policy

1 The Ink Group: Legal Entities

The Ink Group is a trading style of Ink Employee Benefits Ltd (Company Number: 08660956) and Ink HR Ltd (Company Number: 06977572). Ink Employee Benefits Ltd is authorised and regulated by the Financial Conduct Authority (609071).

2 Commitment to Information Security

As a business The Ink Group has always taken data security and privacy extremely seriously - we process a significant volume of personal information on behalf of our clients, and we also control the personal information of our own workforce. We are issuing this Privacy Policy to ensure any third parties who work with us – or who would like to work with us – are assured of our commitment to information security.

Ink HR Ltd is registered with the Information Commissioner's Office under reference No. ZA080262. Ink Employee Benefits Ltd is registered with the Information Commissioner's Office under reference No. ZA096195.

3 Information Security Management System (ISMS)

The Ink 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: contractual agreements; policies and protocols; guidelines and training; ongoing risk assessment.

3.1 Contractual Agreements

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

	Employees	Contractors	Customers
Contract of Employment, with confidentiality and non-disclosure clauses	√		
Service Contract (or equivalent), with confidentiality and non-disclosure clauses		√	
Service Specification Agreement			√
Commercial Terms of Business			√

In addition to the documentation listed above which is issued by The Ink Group, we are required to sign separate Terms of Business Agreement (TOBAs) with all providers with whom we have an agency relationship.

3.2 Policies & Protocols

The Ink 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 breach reporting

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

3.4 Guidelines & Training

The Ink 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.

The Ink Group documents step by step procedural guidelines for its account management tasks and activities. These include services within the Employee Benefits, HR and Payroll workflows.

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

3.5 Risk Assessment

The Ink 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 The Ink 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 have documented evidence of their compliance with GDPR.

5 Physical Security

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

5.1 Premises Access Control

No individual can access our office environment without a key card access during business hours of 8:30am to 5:30pm. Office key holders are restricted only to senior personnel with a register of key holders maintained at all times.

5.2 Server Access Control (Physical)

Server, routers and other business critical equipment is stored securely under locked cover with keypad access restricted to office key holders only.

5.3 Server Access Control (Digitial)

Server access is via Local Area Network (LAN), access to which is controlled by Multi-Factor Authentication (MFA). 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 The Ink Group is subject to encryption and / or password control.

6 Cyber Security

The Ink 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.