



## Statement of Assurance

The General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) is a privacy and data protection regulation in the European Union (EU), enforceable from May 25 2018 and requires no enabling legislation so automatically becomes binding and applicable on that date.

The GDPR imposes new obligations on organisations that control or process relevant personal data and introduces new rights and protections for EU data subjects.

The GDPR applies to data processing carried out by organisations operating within the EU. It also applies to organisations outside the EU that offer goods or services to individuals in the EU.

Dataquest UK Ltd places a high importance on information security. This includes our intellectual and employee data, as well as that of our customers and their clients where appropriate.

Dataquest UK will be complying with the GDPR as a processor and controller of data and have been planning and developing a programme of works to deliver what is required by the legislation. This has involved working with our suppliers and partner organisations to ensure they can meet these obligations.

Key Dataquest personnel have undergone specific security training to help harden our security practices and integrate

them into our ISO business processes manual. Dataquest has also engaged an external advisor to ensure we deliver best practice in compliance with a view to delivering further BSI accreditation.

- Policy Development: we will review/ refresh and develop our range of policies including (but not limited to) our Information Security Management System, Acceptable Use Policy, Security Controls, Data Breach Policy, Data Asset registry and Business Continuity Plans,
- Privacy Policy: we will provide an updated framework and privacy policy to incorporate the GDPR obligations. This will include legal framework gap analysis arising from the reviews we undertake as the plan progresses.
- Data Impact Assessments & Data Inventory: we are already undertaking a systematic review of the data we store, manage, maintain, collect, process and control. This includes offline storage and paper records. Assessments of the data will review information flow, any data transfers, risk reviews, and structural position in relation to Lawfulness, Purpose, Minimisation, Accuracy, Consent, Limitation, Integrity & Confidentiality, Record Keeping and Accountability.
- Training & Awareness: has been undertaken by all employees. Our employee on-boarding process also incorporates contractual obligations and mandatory training specifically designed around meeting GDPR responsibilities. Our management and marcoms teams continue to provide regular security insights and information to users, keeping compliance fresh in their minds.
- Controls & Gap Analysis: running alongside the work already underway, we are auditing our security

continuously both internally and with external consultants. These audits and findings are part of our Management committee quality review meetings.

- Supplier & Partner relationships: where relevant and related, we will be using all reasonable endeavours to ensure that our third party and suppliers are complying with the GDPR.
- Technology: we will be reviewing our technology platforms to analyse their operation, security, compliance in order to ensure that they meet the standards we have laid down and identify any gaps and risks.

Where clients provide Dataquest UK with data assets of any type (personal or not,) we work with them in line with their statement of applicability and security policies, to provide risk assessment and controls to mitigate that risk.

