RSC Associates Limited
GDPR Statement of Compliance
March 2018

1 Introduction
This statement of compliance sets out how RSC Associates Limited, hereafter referred to as RSC, complies with the General Data Protection Regulation (EU) 2016/679 (GDPR).

2 Scope
The scope of RSC's GDPR compliance is geared to our role as a Data Processor to our Clients, as well as being a Data Controller. The scope applies to all RSC operations and services involving the handling of personal data concerning an identified or identifiable natural person, this includes the following activities:

- Document storage, collection and retrieval
- Conversion of data from hard copy to digitised form
- The provision of electronic archiving
- Confidential shredding

Please note that in our role as Data Processor and while acting on behalf of you the Data Controller, this statement of compliance references some Data Controller responsibilities and assumes that as Data Controller you are fulfilling your obligations under GDPR as Data Controller, and specifically as stated in 3.1.3 below.

3 Statement of Compliance
RSC has implemented the following measures to ensure full compliance with GDPR and to protect all personal data that we process from accidental or unlawful destruction, loss, alteration, access or disclosure.

3.1 General Technical and Organisational Information Security Measures	
3.1.1	We have updated our terms and conditions and we are in the process of issuing new contracts and schedules of work to our Clients to ensure compliance to GDPR for both our Client as the Data Controller and RSC as the Data Processor. All services involving the handling of personal data are clearly identified in these new schedules. Please refer to our updated terms and conditions.
3.1.2	All RSC policies, procedures and processes are in the process of being reviewed and updated for GDPR compliance, including our roles as Data Processor and Data Controller and incident/breach management.
3.1.3	We will process personal data only in accordance with the Data Controller's written instructions which shall be in line with their

	specified purpose(s), their legal basis of processing and all other principles stated in paragraph 1 (a-f), Article 5 of the GDPR. If we need to change the way that we process personal data, we will only do this through a formal change request process and after obtaining written permission from authorised users.
3.1.4	We will assist the Data Controller in meeting the requirements of GDPR with regard to the notification of personal data breaches and data protection impact assessments.
3.1.5	Information security is embedded in all RSC policies, processes and procedures.
3.1.6	We are in the process of investigating the actions that will be required to achieve ISO 27001:2013 (Information Security) certification by a UKAS accredited certification body. Such certification is closely aligned to the requirements of GDPR and will further demonstrate that our buildings, infrastructure, systems, policies, processes, procedures and controls are adequately robust to protect all personal data that we process.

3.1.7	We have carried out a data audit and produced a full record of our processing activities which is compliant with Article 30, GDPR 2016.
3.1.8	We operate an integrated risk management framework. We regularly assess and manage the risks associated with protecting the confidentiality, integrity and availability of the personal data that we process and their related assets.
3.1.9	On written instruction from the Data Controller, we can securely destroy any data no longer required or has passed its retention period quickly and easily.
3.1.10	Our site and our processes are regularly audited by our Clients for adherence to the Data Protection Act 1998 and GDPR and with no major issues found. We will contribute to reasonable audits and inspections required by the Data Controller. The scope and timelines of such audits will be agreed with the Data Controller in writing and in advance.
3.1.11	We are conducting internal audits to validate that we are GDPR compliant and to identify any further areas for improvement.
3.1.12	We have robust business continuity and disaster recovery plans in place to minimise the impact of any disruptive incidents or disasters, and our systems and processes are resilient enough to protect the confidentiality, integrity and availability of personal data.

3.1.13	We regularly test our business continuity / disaster recovery plans to ensure we can quickly restore our operations in the event of a disaster or incident.
3.1.14	We follow the guidelines detailed in BS 10008 which describes how information should be managed to ensure that it is available, accessible, demonstrably trustworthy and admissible as legal evidence. We are planning to have our operational controls and processes further independently audited by an expert in the legal admissibility of electronic records.
3.1.15	We have a designated Data Protection Officer (DPO) who monitors our compliance to GDPR and is the central point of contact with the regulator (the ICO).

3.2 RSC Systems and Hardware	
3.2.1	All our internal and external end-user systems have been developed to ensure that they are fully GDPR compliant; this includes the recording of all user activity and additional functionality to assist our Clients with managing document retrieval, retention and deletion.
3.2.2	Our systems enable us to fulfil our obligations for a data subject's right of access to, rectification of or restriction of personal data. All personal data is backed up, and this is encrypted and stored securely. We will inform the Data Controller of any requests or complaints that we receive from a data subject regarding the exercising of their rights under GDPR.
3.2.3	Our systems enable us to fulfil our obligations for the '**Right to be Forgotten**' (Article 17, GDPR 2016). Personal digital data can be securely and fully removed from our systems. Personal physical data can be securely destroyed on receipt of a written request from authorised users.
3.2.4	Our systems enable us to fulfil our obligations for the '**Right to Data Portability**' (Article 20, GDPR 2016). All personal data can be exported from our systems by authorised Client users on a self-service basis or we can physically move personal data to an alternative location on receipt of a written request from authorised users.
3.2.5	Personal data is encrypted at rest on our servers as well as in transit. All RSC servers are located the UK.
3.2.6	Disaster recovery is in place for our critical systems and is regularly tested.

3.2.7	All laptops and desktops run the latest security patches and antivirus software. They are also encrypted and contain personal firewalls

3.3 Supply Chain	
3.3.1	We operate a preferred supplier policy – suppliers are only approved and used after they have passed a strict application and vetting process.
3.3.2	We audit our suppliers for adherence to the Data Protection Act 1998 and GDPR.
3.3.3	We ensure that all our suppliers who may have exposure to confidential information have signed confidentiality/non-disclosure agreements.
3.3.4	We will only engage sub-processors after receiving prior written consent from the Data Controller and under a written agreement with the sub-processor and includes data protection obligations that meet the requirements of GDPR.

3.4 Staff Education, Awareness and Integrity	
3.4.1	GDPR and information security training and awareness is included in our company induction for all new employees.
3.4.2	All existing members of staff have received training on their responsibilities for GDPR, and this is ongoing. They also receive annual training on their roles and responsibilities for information security.
3.4.3	All staff who are authorised to process personal data do so on a strictly 'need-to-know' basis and as necessary to perform their role in the provision of required services.
3.4.4	All RSC staff have signed a confidentiality/non-disclosure agreement which forms part of their contract of employment.

4 Declaration

4.1 RSC Declaration (the Data Processor)
We confirm that the above measures are in place. These measures are monitored for their continued suitability and adequacy for compliance with GDPR.
Ian Martin
Managing Director
RSC Associates Limited
1st March 2018