RGA UK Ltd: GDPR Supplier Security Assessment Questionnaire

This SSAQ has been issued by RGA UK Ltd to serve as a preliminary assessment of the security controls provided as part of the requested service. RGA Terms & Conditions / Privacy Policy

Supplier Name & Address	RGA UK Ltd, RGA Centre, Holwell, Oxfordshire. OX18 4LD
Supplier Telephone	01993 822303
UK Registration Number	3902620
VAT Registration	718 3350 41
ICO Number	Z4981496
Web address	www.rgaukltd.co.uk
Number of Employees	6
Assessment Completed by	Gwyneth Gibbons, Managing Director
Date of Assessment	20 August 2018

1 - Personal Data Held

	Question	***RGA: yes / no***
Databases	Do you supply any databases to our organisation containing **personal data** such as mailing lists, job applicants, training records etc	yes

2 – Scope

	Question	***RGA: yes/no***
Main establishment	Is your head office based outside the UK/EU?	no
Joint processors	Are there any joint data processing relationships, i.e. subcontractors, who undertake work on your behalf to enable you to meet your contractual relationship with us?	no
Sensitive (special) personal data	Are you processing any sensitive personal data on our behalf?	no

3 - Data Security

	Question	***RGA***
Appropriate technical and organisational security	Are the risks inherent in the processing formally evaluated, tested and assessed?	yes
	Have measures to mitigate those risks and ensure the security of the processing been implemented?	yes
	Is there a documented security programme that specifies the technical, administrative and physical safeguards for personal data?	Cyber Essentials – application pending
	What is the time interval at which security policies are reviewed and updated	annually
	Is there a documented process for resolving security related complaints and issues?	yes
	Is there a designated individual who is responsible for driving remediation plans for security gaps?	Raymond Gibbons
	Are industry standard encryption algorithms and technologies employed for transferring, storing, and receiving individuals' sensitive personal information?	yes
	Is personal information systematically destroyed, erased, or anonymised when it is no longer legally required to be retained or to fulfil the purpose(s) for which it was collected?	yes
	Are steps taken to pseudonymise personal data where possible?	yes
	Can the availability and access to personal data be restored in a timely manner in the event of a physical or technical incident?	yes
	Do terms and conditions of employment clearly define information security requirements	yes

4 - Data Breaches

	Question	***RGA***
Breach response obligations	Does the organisation have a documented privacy and security Incident Response Plan and any incident identification systems?	yes
	Are the plan and procedures regularly reviewed and road tested?	yes
	Are there procedures in place to notify the ICO and data subjects of a data breach (where applicable)?	yes
	Is there clear internal guidance explaining when notification is required and what information needs to be reported?	yes
	Are there clear procedures in place to notify the controller in the prescribed form of any data breach without undue delay after becoming aware of it?	yes
	Are data breaches documented?	yes
	Are there cooperation procedures in place between controllers, suppliers and other partners to deal with data breaches?	yes

5 - Lawful Grounds For Processing

	Question	***RGA***
Lawful grounds for processing	What are the lawful grounds for processing the personal data for each processing operation?	Consent & Legitimate Interest
Consent	How is consent collected?	Direct communication with data subject
	How is this consent demonstrated?	Registered on internal database
	Can subjects withdraw their consent?	yes

6 - Transparency Requirements

	Question	***RGA***
Source of personal data and information provided to data subject	Is data collected directly from the subject and is the required information given to them?	yes

7 - Data Subject Rights

	Question	***RGA***
Access to personal data	Is there a documented policy/procedure for handling subject access requests?	yes
	Are individuals provided with a mechanism to request access to information held about them?	yes
	Is the data controller able to respond to SARs within one month?	yes
Erasure and rectification	Are individuals informed of their right to demand erasure or rectification of personal information held about them (where applicable)?	yes
	Are there controls and formal procedures in place to allow personal data to be erased or blocked?	yes
Right to object	Are individuals told about their right to object to certain types of processing?	yes
Profiling and automated processing	Is profiling based on consent? (if so this must be explicit).	No profiling is undertaken by RGA
	Does any profiling use sensitive data?	no

8 - International Personal Data Transfers

	Question	***RGA***
International data flow mapping	Is personal data transferred outside the EEA?	no

9 - Other Processor Obligations

	Question	***RGA***
Use of sub-processors	Is there written authorisation for existing sub-processing arrangements?	No sub processors or sub processing
	Is sensitive personal data processed?	No sensitive data is processed or held by RGA UK Ltd
	Are the legal grounds for processing personal data recorded?	yes
Data Protection Officer (DPO)	Do you have or do have a DPO?	Raymond Gibbons
Assistance to data controller	Are you able to assist the data controller in ensuring compliance under the GDPR?	yes

I certify that to the best of my knowledge that the information provided is correct:

Name: Gwyneth Gibbons

Signature:

Date: 17/08/2018