GDPR Data Processing Agreement

Document Reference
GDPR/DataProcessingAgreement

Revision Date
28th Mar 2017

Revision Number
001

Paritor Ltd,
Ground Floor, Compton House
11 Park5, Exeter, Devon EX2 7HU
01395 445092
info@paritor.co.uk
www.paritor.com

Data Processing Agreement

This **Paritor Ltd** Data Processing Agreement addendum ("**Paritor Ltd** Addendum") is entered into between the parties identified on the signature form for the Enrolment identified above ("Enrolment"). The parties agree that the **Paritor Ltd** Addendum supplements the Enrolment and applies to only the Platform Services, defined in the Enrolment.

Defined Terms

Capitalised terms used but not defined in this **Paritor Ltd** Addendum will have the meanings provided in the Enrolment, Enterprise Agreement, and applicable **Paritor Ltd** Business Agreement/**Paritor Ltd** Business and Services Agreement. The following definitions are used in this **Paritor Ltd** Addendum:

"Customer Data" means all data, including all text, sound, or image files that are provided to **Paritor Ltd** by, or on behalf of, Customer through Customer's use of the Platform Services.

"Core Platform Services" include Windows Azure Compute, Storage, Virtual Machines, Connect, and Traffic Manager. It does not include at this time Windows Azure Content Delivery Network, Access Control, Caching, Service Bus, or SQL Azure.

1. Privacy.

a. Privacy practices. The company complies with all data protection and privacy laws generally applicable to the company's provision of the Platform Services. However, the company is not responsible for compliance with any data protection or privacy law applicable to Customer or its industry and not generally applicable to information technology service providers.

b. Customer Data. The company will process Customer Data in accordance with the provisions of this agreement and, except as stated in agreement, the company (1) will acquire no rights in Customer Data and (2) will not use or disclose Customer Data for any purpose other than stated below. The company's use of Customer Data is as follows:

(i) Customer Data will be used only to provide Customer the Platform Services. This may include troubleshooting aimed at preventing, detecting and repairing problems affecting the operation of the Platform Services and the improvement of features that involve the detection of, and protection against, emerging and evolving threats to the user (such as malware or spam).

(ii) The Company will not disclose Customer Data to a third party (including law enforcement, other government entity, or civil litigant; excluding our subcontractors) except as Customer directs or unless required by law. Should a third-party contact the Company with a demand for Customer Data, the Company will attempt to redirect the third party to request it directly from Customer. As part of that, the

Company may provide Customer's basic contact information to the third party. If compelled to disclose Customer Data to a third party, **Paritor Ltd** will use commercially reasonable efforts to notify Customer in advance of a disclosure unless legally prohibited.

c. Customer Data deletion or return. Upon expiration or termination of Customer's use of the Platform Services, Customer may extract Customer Data and the Company will delete Customer Data, each in accordance with the use rights for the Platform Services.

d. End User requests. The Company will not independently respond to requests from Customer's End Users without Customer's prior written consent, except where required by applicable law.

e. Transfer of Customer Data; appointment. Customer Data that the Company processes on Customer's behalf may be transferred to, and stored and processed in, the EU. Customer appoints the Company to perform any such transfer of Customer Data to any such country and to store and process Customer Data in order to provide the Platform Services.

f. Company personnel. The Company personnel will not process Customer Data without authorisation. The Company personnel are obligated to maintain the confidentiality of any Customer Data and this obligation continues even after their engagement ends.

g. Subcontractor; transfer. The Company may hire other companies to provide limited services on its behalf, such as providing customer support. Any such subcontractors will be permitted to obtain Customer Data only to deliver the services the Company has retained them to provide, and they are prohibited from using Customer Data for any other purpose. The Company remains responsible for its subcontractors' compliance with the obligations of this agreement. Any subcontractors to whom the Company transfers Customer Data will have entered into written agreements with the Company requiring that the subcontractor provide at least the same level of privacy protection with respect to personal data received from the Company. Customer consents to the Company transfer of Customer Data to subcontractors as described in this agreement. Except as set forth above, or as Customer may otherwise authorise, the Company will not transfer to any third party (not even for storage purposes) personal data Customer provides to the Company through the use of the Platform Services.

2. Customer responsibilities.

Customer must comply with applicable legal requirements for privacy, data protection, and confidentiality of communications related to its use of Platform Services. Customer is wholly responsible for implementing and maintaining privacy protections and security measures within any applications provided by Customer, or on Customer's behalf, for use in the Platform Services.

a. Intent of the parties. For the Platform Services, Customer is the data controller and the Company is a data processor acting on Customer's behalf. As data processor, the Company will only act upon Customer's instructions. This agreement is the Customer's complete and final instructions to the Company for the processing of Customer Data. Any additional or alternate instructions must be agreed service contract.

b. Duration and object of data processing. The duration of data processing shall be for the term designated under the service contract. The objective of the data processing is the performance of the Platform Services.

c. Scope and purpose of data processing. The scope and purpose of processing of Customer Data, including any personal data included in the Customer Data, is described in this agreement.

d. Customer Data access. For the term designated under the Service Contract the company will provide Customer with the ability to correct, delete, or block Customer Data.

e. Data Protection Officer. The Company's data protections officer can be reached at the following address:

Paritor Ltd
Data Protection Officer
Ground Floor, Compton House, 11 Park5, Harrier Way, Exeter, Devon EX2 7HU

3. Security.

a. General practices. The Company has implemented and will maintain for the Platform Services appropriate technical and organisational measures, internal controls, and information security routines intended to protect Customer Data against accidental loss, destruction, or alteration; unauthorised disclosure or access; or unlawful destruction. Customer is wholly responsible for implementing and maintaining security within any applications provided by Customer, or on Customer's behalf, for use in the Platform Services.

b. Core Platform Services. For Core Platform Services, The Company has implemented and will maintain the following:

(i) Domain: organisation of information security.

1) Security ownership. **Paritor Ltd** has appointed one or more security officers responsible for coordinating and monitoring the security rules and procedures.

2) Security roles and responsibilities. **Paritor Ltd** personnel with access to Customer Data are subject to confidentiality obligations.

3) Risk management program. **Paritor Ltd** performed a risk assessment before processing the Customer Data or launching the Core Platform Services.

4) **Paritor Ltd** retains its security documents pursuant to its retention requirements after they are no longer in effect.

(ii) Domain: asset management.

1) **Asset inventory.** **Paritor Ltd** maintains an inventory of all media on which Customer Data is stored. Access to the inventories of such media is restricted to **Paritor Ltd** personnel authorised in writing to have such access.

2) **Asset handling.**

A. **Paritor Ltd** restricts access to Customer Data. Customer may implement encryption of Customer Data within Customer's application. **Paritor Ltd** imposes restrictions on printing Customer Data and has procedures for disposing of printed materials that contain Customer Data.

B. **Paritor Ltd** personnel must obtain **Paritor Ltd** authorisation prior to storing Customer Data on portable devices, remotely accessing Customer Data, or processing Customer Data outside of **Paritor Ltd** facilities. This includes removing media (e.g., USB sticks and CD ROMs) and documents containing Customer Data from the **Paritor Ltd** facilities.

(iii) **Domain: human resources security.**

1) **Security training.**

A. **Paritor Ltd** informs its personnel about relevant security procedures and their respective roles. **Paritor Ltd** also informs its personnel of possible consequences of breaching the security rules and procedures. **B. Paritor Ltd** will only use anonymous data in training.

(iv) **Domain: physical and environmental security.**

1) **Physical access to facilities.** **Paritor Ltd** limits access to facilities where information systems that process Customer Data are located to identified authorised individuals.

2) **Physical access to components.** **Paritor Ltd** maintains records of the incoming and outgoing media containing Customer Data, including the kind of media, the authorised sender/recipients, date and time, the number of media and the types of Customer Data they contain.

3) **Protection from disruptions.** **Paritor Ltd** uses a variety of industry standard systems to protect against loss of data due to power supply failure or line interference.

4) **Component disposal.** **Paritor Ltd** uses industry standard processes to delete Customer Data when it is no longer needed.

(v) **Domain: communications and operations management.**

1) **Operational policy.** **Paritor Ltd** maintains security documents describing its security measures and the relevant procedures and responsibilities of its personnel who have access to Customer Data.

2) **Data recovery procedures.** The Platform Services include replication features that facilitate recovery of Customer Data in the event a particular machine or cluster within a **Paritor Ltd** data centre fails. Customers are responsible for taking

additional steps to provide added fault tolerance, such as creating historical backups of Customer Data, storing backups of Customer Data off the platform, deploying redundant compute instances within and across data centres, or backing up state and data within a virtual machine.

A. On an ongoing basis, but in no case less frequently than once a week (unless no Customer Data has been updated during that period), **Paritor Ltd** maintains multiple copies of Customer Data from which Customer Data can be recovered. **Paritor Ltd** does not preserve state or data within a virtual machine, which will be restored to its original state.

B. **Paritor Ltd** stores copies of Customer Data and data recovery procedures in a different place from where the primary computer equipment processing the Customer Data is located.

C. **Paritor Ltd** has specific procedures in place governing access to copies of Customer Data.

D. **Paritor Ltd** reviews data recovery procedures at least every six months.

E. **Paritor Ltd** logs data restoration efforts, including the description of the restored data, and where applicable, the person responsible and which data (if any) had to be input manually in the data recovery process.

3) Malicious software. **Paritor Ltd** has anti-malware controls to help avoid malicious software gaining unauthorised access to Customer Data, including malicious software originating from public networks.

4) Data beyond boundaries.

A. **Paritor Ltd** provides Customer the option of encrypting Customer Data transmitted to and from **Paritor Ltd** data centres over public networks.

Paritor Ltd uses encryption for replication of non-public Customer Data between **Paritor Ltd** data centres.

B. **Paritor Ltd** restricts access to Customer Data in media leaving its facilities (e.g., through encryption).

(vi) Domain: access control.

1) Access policy. **Paritor Ltd** maintains a record of security privileges of individuals having access to Customer Data.

2) Access authorisation.

A. **Paritor Ltd** maintains and updates a record of personnel authorised to access **Paritor Ltd** systems that contain Customer Data.

B. **Paritor Ltd** deactivates authentication credentials that have not been used for a period of time not to exceed six months.

C. **Paritor Ltd** identifies those personnel who may grant, alter or cancel authorised access to data and resources.

3) **Least privilege.**

A. Technical support personnel are only permitted to have access to Customer Data when needed.

B. **Paritor Ltd** restricts access to Customer Data to only those individuals who require such access to perform their job function.

4) **Integrity and confidentiality.** **Paritor Ltd** instructs **Paritor Ltd** personnel to disable administrative sessions when leaving premises Microsoft controls or when computers are otherwise left unattended.

5) **Authentication.**

A. **Paritor Ltd** uses industry standard practices to identify and authenticate users who attempt to access information systems.

B. Where authentication mechanisms are based on passwords, **Paritor Ltd** requires that the passwords are renewed regularly.

C. Where authentication mechanisms are based on passwords, **Paritor Ltd** requires the password to be at least eight characters long.

D. **Paritor Ltd** ensures that de-activated or expired identifiers are not granted to other individuals.

E. **Paritor Ltd** monitors or enables Customer to monitor repeated attempts to gain access to Customer Data using an invalid password.

F. **Paritor Ltd** maintains industry standard procedures to deactivate passwords that have been corrupted or inadvertently disclosed.

G. **Paritor Ltd** uses industry standard password protection practices, including practices designed to maintain the confidentiality and integrity of passwords when they are assigned and distributed, and during storage.

6) **Network design.** **Paritor Ltd** has controls to avoid individuals assuming access rights they have not been assigned to gain access to Customer Data they are not authorised to access.

(vii) **Domain: information security incident management.**

1) **Incident response process.** **Paritor Ltd** maintains a record of security breaches with a description of the breach, the time period, the consequences of the breach, the name of the reporter, and to whom the breach was reported, and the procedure for recovering data.

2) **Service Monitoring.** **Paritor Ltd** security personnel verify logs at least every six months to propose remediation efforts if necessary.

(viii) **Domain: Business Continuity Management.**

1) **Paritor Ltd** maintains emergency and contingency plans for the facilities in which **Paritor Ltd** information systems that process Customer Data are located.

2) Paritor Ltd's redundant storage and its procedures for recovering data are designed to attempt to reconstruct Customer Data to its last replicated state from before the time it was lost or destroyed. Recovery of virtual machines will be to their original image.

(ix) **Security measures.** The security measures described in this Section 4 are **Paritor Ltd's** only responsibility with respect to the security of Customer Data. For Customer Data, these measures replace any confidentiality obligations contained in the Enrolment or any other nondisclosure agreement between **Paritor Ltd** and Customer.

(x) **Data security policy.** **Paritor Ltd** has established and agrees to maintain a data security policy that complies with the ISO 27001 standards for the establishment, implementation, control, and improvement of the Information Security Management System and the ISO/IEC 27002 code of best practices for information security management ("Windows Azure Information Security Policy"). On a confidential need-to-know basis, and subject to Customer's agreement to non-disclosure obligations **Paritor Ltd** specifies, **Paritor Ltd** will make the Windows Azure Information Security Policy available to Customer, along with other information reasonably requested by Customer regarding **Paritor Ltd** security practices and policies. Customer is solely responsible for reviewing the Windows Azure Information Security Policy, making an independent determination as to whether the Windows Azure Information Security Policy meets Customer's requirements, and for ensuring that Customer's personnel and consultants follow the guidelines they are provided regarding data security.

4. ***Certifications and audits.***

(i) **Paritor Ltd** will audit the security of the computers and computing environment that it uses in processing Customer Data (including personal data) on the Core Platform Services (audit does not currently include non-Core Platform Services) and the physical data centres from which **Paritor Ltd** provides all Platform Services except the Content Delivery Network. This audit: (1) will be performed at least annually; (2) will be performed according to ISO 27001 or other industry standards; (3) will be performed by third party security professionals at **Paritor Ltd's** selection and expense; (4) will result in the generation of an audit report ("**Paritor Ltd** Audit Report"), which will be **Paritor Ltd's** confidential information; and (5) may be performed for other purposes in addition to satisfying this Section (e.g., as part of **Paritor Ltd's** regular internal security procedures or to satisfy other contractual obligations).

(ii) If Customer requests in writing, **Paritor Ltd** will provide Customer with a confidential summary of the **Paritor Ltd** Audit Report ("Summary Report") so that Customer can reasonably verify **Paritor Ltd's** compliance with the security obligations under this **Paritor Ltd** Addendum. The Summary Report is **Paritor Ltd** confidential information.

(iii) **Paritor Ltd** will make good faith, commercially reasonable efforts to remediate (1) any errors identified in a **Paritor Ltd** Audit Report that could reasonably be expected to have an adverse impact on Customer use of the Platform Services and (2) material control deficiencies identified in the **Paritor Ltd** Audit Report.

5. Miscellaneous.

a. **Confidentiality.** Customer will treat the contents of the Windows Azure Information Security Policy, the **Paritor Ltd** Audit Report and the Summary Report as confidential and shall not disclose them to any third party except for Customer's auditors or consultants that need access to this information for the purpose of this business relationship as articulated in this **Paritor Ltd** Addendum and the Enrolment.

b. **Term and termination.** This **Paritor Ltd** Addendum shall automatically terminate upon any termination or expiration of the Enrolment.

c. **Order of precedence.** If there is a conflict between any provision in this **Paritor Ltd** Addendum and any provision in the Enrolment, Enterprise Agreement, or applicable **Paritor Ltd** Business Agreement/**Paritor Ltd** Business and Services Agreement, this **Paritor Ltd** Addendum shall control.

d. **Entire agreement.** Except for changes made by this **Paritor Ltd** Addendum, the Enrolment remains unchanged and in full force and effect.

This Addendum must be attached to a signature form to be valid.