Data Processing Agreement Addendum - Cloud Virtual Machines

Last Updated May 2018

Glossary of terms

- **Applicable Law** : European Union or member state laws with respect to Personal Data processing in respect of which Blacknight as personal data processor is subject to (including EU Directive 95/46/EC, as transposed into domestic legislation of each member state and as amended, replaced or superseded from time to time, including by the EU General Data Protection Regulation 2016/679 (hereinafter GDPR)) and laws implementing or supplementing the GDPR)
- **Client /Customer:** Person or legal entity who has purchased the dedicated server and any associated managed services
- **Personal Data:** any personal data processed by Blacknight on behalf of the Client pursuant to or in connection with the Contract
- **The terms**,"Processor", "Controller", "sub-processor" "transfer of data", "Data Subject", "Personal Data" shall have the same meaning as in the GDPR and shall be construed accordingly.
- **Sub-processor**: Vendor partner of Blacknight who may from time to time be called upon to provide support on the product or platform. (e.g. Plesk, cPanel, OnApp, R1Soft, Acronis, etc.)
- **Retention**: The archiving or retention of data as agreed between the parties.
- **Cloud Virtual Machine** – A virtual instance of a server deployed via a template chosen by the customer which determines the Operating system and resources available. A virtual machine is an emulation of a physical server which provides the functionality of a physical server.
- **Managed Services** – add-on services to the dedicated server package, which require access to the server by Blacknight employees, for the purpose of configuring those services (e.g. Backup software)

This document is intended to be supplementary to the existing "General Terms of Service" agreement as published on www.blacknight.com/legal/terms for the purpose of providing a Data Processing Agreement specific to Cloud Virtual Machines (VMs)

DATA PROCESSING ADDENDUM

1. Blacknight will act as a data processor on behalf of the client by providing the underlying platform or infrastructure for deploying virtual machines which will have access to the public internet via our edge network infrastructure and Blacknight will only process data on specific written instruction from the authorized representative of the client (via a helpdesk ticket submitted by email to support@blacknight.com) Blacknight are also a processor where the client has subscribed to Managed Services solely in that it may manage software, backups, security patches or other aspects of the services agreed to. Blacknight will not process the client's actual data unless specifically requested in the process of troubleshooting the platform.
2. In order to provide the service and to perform support troubleshooting, by default Blacknight engineers will have access to the cloud Virtual Machines via an SSH key or will have access to the passwords displayed in the control panel. This can be removed by the customer and the customer can remove all access by resetting the password and removing the SSH key where applicable.

3. The client is deemed to be the data controller of any data stored on the Cloud Virtual Machine and associated backups.
4. Blacknight may use network diagnostic tools such as packet traces or TCP dumps (this list is not exhaustive), on traffic to or from the cloud virtual servers only when necessary to protect the network and other customers from DDoS, or other malicious attacks and may at its sole discretion disable such traffic or suspend the virtual server if is deemed to be malicious.
5. Blacknight may request its vendor partners (OnApp, SolidFire Storage) to assist in troubleshooting platform or Virtual machine related issues where necessary, but will inform and seek permission from the client in such cases. The client has the right to refuse access by any 3rd party on the understanding that Blacknight may not be able to meet its service obligations and as such understands that the Client will be solely responsible for any damage or liability resulting from failure to deal with any platform related issues where consent has requested by Blacknight and same has not been forthcoming.
6. Blacknight will ensure that any partner vendors have contractually agreed to meet their GDPR obligations and Blacknight will monitor and control any access to the client's servers where possible.
7. Blacknight will ensure that its staff members are security-screened, and competent to provide the services agreed to.
8. Blacknight will assist in providing the client with Data Subject access requests in so far as it will provide access on instruction from the client.
9. Blacknight will assist in the client meeting its GDPR obligations as they pertain to breach notifications only by providing the client with the details available to Blacknight for breach notifications.
10. Blacknight agree to securely store and then delete all data from disks or any storage media in a controlled fashion within 1 year, by using its current "disk destruction" process under ISO27001, unless a specific retention period has been otherwise formally agreed with the client. Backup disk safes will be deleted within 3 months and can be made available (for an agreed fee and prior to deletion) to the client for data portability purposes.
11. Blacknight agree to submit to reasonable audits or inspections from the client and reserve the right to charge a fee for such audits which will be in line with our professional services charges. Requests for audits must be limited to once in a calendar year.