Data Processing Agreement – Co-Location Services

Last Update 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EU Directive 95/46/EC, as transposed into domestic legislation of each member state and as amended, replaced or superseded from time to time, including by the EU General Data Protection Regulation 2016/679 (hereinafter GDPR)) and laws implementing or supplementing the GDPR)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:** Person or legal entity who has purchased the colocation services 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.
- **Colocation Services –** the provision of Rackspace, power and network connectivity to a client for the purpose of hosting their IT equipment in a designated data centre.
- **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)
- **DDoS** – distributed denial of service (a malicious external attempt to deny public access to public facing internet services)

This document is supplementary to existing colocation contracts / agreements in place up to May 24th 2018 to allow for the provision of a Data Processing Agreement (processor to controller) specific to Colocation contracts.

DATA PROCESSING ADDENDUM

1. Blacknight will act as a data processor on behalf of the client by providing colocation services and access to the public internet via our core and edge network infrastructure. Blacknight engineering staff or data centre staff may have physical access to the equipment for the purpose of maintaining service level agreements with regard to power and network connectivity uptime. The client may subscribe to our firewall services or other network security features (such as DDoS mitigation) and in this case Blacknight is considered a joint-controller for those services only as it manages network access to the equipment. Blacknight manage firewall requests

under change control to record any changes to firewall rules requested by the client.

2. The client is deemed to be the data controller of any data stored on the co-located equipment and associated storage unless otherwise mutually agreed, Blacknight staff are not authorized to access or connect to such equipment without the written consent of the client, such consent not to be unreasonably withheld or delayed..
3. Blacknight may use network diagnostic tools such as packet traces or TCP dumps (this list is not exhaustive), on traffic to or from the collocated equipment (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 if is deemed to be malicious.
4. Blacknight will reasonably ensure the racks where the client equipment is located are physically secured and any access to the client's equipment is recorded and controlled. Blacknight will perform audits of physical access to the data centre suite, and will maintain a record of requests for physical access to the customers collocated equipment.
5. Blacknight will ensure that its staff members are security-screened to provide the services agreed to and are made of aware of their compliance obligations under GDPR
6. Blacknight will reasonably assist in providing the client with Data Subject Access Requests in so far as it will provide available log-files with regard to physical or logical access where available.
7. Blacknight will assist in the client meeting its GDPR obligations as they pertain to breach notification by providing the client with relevant information held by Blacknight in the event of a security breach and will notify the Client in accordance with GDPR timelines.
8. Blacknight agree to return any equipment belonging to the Client on termination of the contract once all contract obligations have been fulfilled by the client, but reserve the right to withhold access to the equipment or data until any financial or billing disputes have been resolved to the satisfaction of both parties.
9. Blacknight agree to submit to reasonable audits or inspections from the client, (or to accommodate third party audits at the request of 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.