



GDPR Compliance Responsibilities on Blacknight Products

April 2018

We're on
TRUSTPILOT



Our customers love us!



Taking care of *Irish* business since 2003

GDPR is due to come into force May 25th 2018. It sets out regulations for security and privacy controls required when handling Personally Identifiable Data (PII). This document attempts to clarify the responsibilities of both Blacknight and the Customer for the various platform services, which Blacknight provides.

Blacknight offer domain registrations, shared hosting, Cloud servers, dedicated & co-located servers, hosted mail (Q-mail, Hosted Exchange) and Office 365 platforms for customers to host their data with us. Each platform type is different and whilst we control the platform, we do not have visibility on a customer's data and therefore we are not always considered to be a data controller under GDPR regulations. As this document attempts to clarify, Blacknight have full responsibility for managing the security and integrity of the platform, shares responsibility with regard to data protection in some cases, and in other areas, the customer is completely responsible as the data controller.

Domain Registrations

Blacknight register domain registrations on behalf of its customer with various registries or registry resellers (registrars). The data collected by Blacknight is a requirement of the registration process and some of this data is used in populating the WHOIS database, which provides transparency of domain registration globally. Most of this is publicly available information and can be retrieved via a WHOIS query. Blacknight do not control this data, and collection of this data is a requirement under ICANN contractual obligations or the specific policies and contractual requirements imposed by the domain registries. (*Internet Corporation for Assigned Names and Numbers*) **

Shared Hosting

Blacknight provide a range of Shared Hosting services, which allow a customer to provision a website, store database information, and host their email accounts on shared servers (Servers that share resources with other customers). The responsibility for securing the data is therefore shared between Blacknight and the customer. Blacknight are responsible for securing the shared hosting infrastructure (the underlying hardware and operating systems) supporting the platform whilst the content, passwords, access to the data etc. is the responsibility of the customer. In addition, the customer is responsible for their own backups and for securing the CMS applications by keeping them up to date.

Office 365 and Hosted Exchange

Office 365 is Microsoft's online cloud platform mail service, which Blacknight resell through our control panel. We only manage the Office365 accounts via our control panel integration on behalf of Microsoft. The email data is hosted on data centres situated within the EU. Office365 offers solutions to protect customer data such as lockbox, threat management and data loss prevention on specific versions to enhance security and data protection.

Hosted Exchange accounts on the Odin platform are managed by the control panel admin (customer) whilst the mailboxes are stored on Blacknight servers within Ireland.

***This is currently under review with ICANN*

SSL Certificates

Blacknight are authorised resellers of SSL certificates and we collect PII information (name email address, CRO number etc.) pertaining to the certificate to provide the SSL provider with the information necessary to validate the registrant. Where our support team have been requested to provide assistance in the installation of an SSL cert, we store any generated CSR (cert signing request) or private keys in an encrypted database.

BaseKit siteBuilder

BaseKit is a third party site-builder platform, which is available through the Blacknight control panel. This is a cloud based product hosted by BaseKit themselves and similar to how Office 365 accounts are managed via our control panel integration. The data is stored on Base-Kit servers not on Blacknight servers. The account details are maintained in the Blacknight control panel database and a reference ID with domain name is sent to BaseKit.

Cloud Server Virtual Machines

NIST (National Institute for Standards and Technology) defines three primary cloud service delivery mechanisms: infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS).

Blacknight cloud service can be categorised as either PaaS or IaaS depending on the solution. Blacknight are responsible for maintaining the security of the Hypervisor infrastructure, Cloud control panel, infrastructure backups etc. whilst the customer is responsible for the virtual machine (VM) content, for backing up, securing and classifying that content.

Physical security of the data is the one responsibility that is wholly owned by cloud service providers when using cloud-computing models.

With an IaaS service model, for capabilities such as virtual machines, storage, and networking, it's the customer's responsibility to configure and protect the data that is stored and transmitted. When using an IaaS-based solution, data classification must be considered by the customer at all layers of the solution.

The remaining responsibilities are shared between customers and cloud service providers. Some scenarios require Blacknight and the customer to manage and administer the responsibility together, (e.g. in a managed services scenario, Blacknight are responsible for the patching and maintenance of the operating system, whereas the customer is responsible for the configuration of the Operating System and its baseline security). In this scenario, the customer is accountable to ensure their solution and its data is securely identified, labelled and correctly classified to meet any compliance obligation.

Network control - includes the configuration, management, and securing of network elements such as virtual networking, load balancing, DNS, and gateways. The controls provide a means for services to communicate and interoperate. This is Blacknight's responsibility as it is outside the control of the customer.

In an IaaS solution, the customer shares responsibility with a service provider to deploy, manage, secure, and configure the networking solutions to be implemented. (e.g. IP tables or Microsoft Windows firewall rules)

Dedicated Servers

Similar to the cloud services, Blacknight provide dedicated servers for configuration by the customer. The customer leases and has full control of the server and can if necessary remove all access from Blacknight staff. In this instance, the customer has full responsibility for the data and content, whilst Blacknight are responsible for securing physical access to the servers, and where applicable ensuring external firewalls are managed securely.

Managed dedicated servers

In order to manage the server, Blacknight require access to it via SSH key or admin password. In this instance, Blacknight has a responsibility to ensure there is no unauthorised access outside of the Blacknight engineering team and that access is recorded and/or consent is sought prior to access.

Managed private cloud

Similar to Managed dedicated servers, managed private cloud require access to the servers which host the virtual machines (VM) and in some cases to the actual VMs themselves.

Responsibility for the security and classification of data on the VMs is with the customer, and Blacknight is responsible for ensuring restricted authorised access to either the VMs or the Host hypervisors.
























































Co-located Servers

The customer is fully responsible for the configuration, patching and security of any co-located equipment hosted with us. Blacknight are solely responsible for ensuring the service level agreements are met in relation to power and connectivity. Blacknight do not have access to this equipment other than physical access to the rack. Blacknight's sole responsibilities in relation to GDPR therefore, are to ensure physical access to the server is restricted to authorised personnel.

Backup services (Acronis /CDP)

The customer is responsible for ensuring the security of any passwords /URLs provided for access to the Backup portals. Blacknight is responsible for implementing operational controls to restrict authorised access to the backup servers and data.

Data Control Overview

	Domains	Shared Hosting	Cloud	Dedicated & Colo	Online Backup	Managed Servers / Firewalls	Office 365	Hosted Email
Data Classification								
End-Point Protection							 Microsoft	
Identity & Access Management								
Application Level Control								
Network Controls								
Host Infrastructure								
Physical Security								
Legend	Blacknight		Customer		Shared		Microsoft	