DATA PROTECTION STATEMENT

Introduction

Blacknight Internet Solutions Ltd. are a hosting company based in Ireland, currently providing a range of hosting services including Domain registration, shared hosting platforms, email platforms, SSL certs, dedicated hosting, co-location, Cloud services, IP transit, backup services & network services, and are therefore required to comply with EU general data protection regulations (GDPR) from May2018.

Blacknight are certified to ISO 27001:2013 (Information Security) since January 2016 and undergo bi-annual external audits to maintain that certification. The ISO 27001:2013 standard provides our customers with a level of assurance that Blacknight takes the management of Information Security seriously and this document outlines our commitment to apply the same rigorous standards to Data Protection and Data Privacy in accordance with GDPR in the absence of any current Data Privacy compliance standards. We have been implementing a Data Protection Management System (DPMS) since May 2017, which incorporates

- Data Protection Impact Assessment.
- Data Map of data we manage or process.
- Matrix of responsibility (outlining where we are data controller, joint controller or data processor
- Data Classification procedures.
- Policies and procedures in relation to the processing and retention of Personally Identifiable Information (PII) and the processing of special categories of information as outlined in GDPR.
- Policies regarding data minimisation
- Policies and procedures in relation to a data subject's rights of access, erasure, rectification, portability and transparency.
- Procedures in relation to Security Incident handling and breach reporting.
- A staff awareness program on Data Protection

Blacknight's DPMS is managed in conjunction with ISO by the technical manager.
Any request for information, or data subject access requests should be made to gdpr@blacknight.com

Blacknight are currently registered with the office of the Irish Data Protection Commissioner as a Data Processor ref. no. 8053/a.

Blacknight only collects and retains data about individuals or organisations with our customers consent and for the services we offer and for billing purposes via the online website, control panels, and e-commerce site, or where provided directly by the end user for the purpose of contracting for the services we offer. Our customers who utilise those services may also collect and retain data (PII) for their own purposes and should refer to the "Matrix of Responsibility" document (which is published separately), for information on their own GDPR responsibilities.

In accordance with the following GDPR principles, this document sets out to outline in brief how we align our DPMS with those principles.

- Lawfulness, fairness and transparency
- Purpose limitation.
- Data minimisation.
- Accuracy.
- Storage limitation (data retention)
- Integrity and confidentiality.
- Accountability.

DATA PROTECTION POLICY

1.1 Lawfulness, fairness and transparency

Blacknight collects personal information solely for the purpose of providing the services we offer and for billing and accounting purposes. At each point of collection, we will endeavor to provide full transparency as to the purpose, retention, transfer and use of such data.

1.1.1 Domain registration: In order to process and validate domain registrations there may be a requirement to collect additional personal information such as utility bills, passport, drivers licence, CRO details etc. This is a requirement of the registry in question and that data is then forwarded to the registry by Blacknight as part of the application process. We then purge any such data from our own systems within 1 calendar month. All current "thick" domain registry applications require an email address, applicant name, applicant address, country of origin, phone number as part of the registration process and this information is made widely available in the public WHOIS database. This is a contractual requirement of the governing body ICANN, but is currently being reviewed by a number of interested parties including the EU commission, registries and registrars. WHOIS privacy can be used to obfuscate that information from the public WHOIS datastore.

1.1.2 Fraud Prevention: In order to circumvent fraud when registering for our products, we have policies in place to validate orders outside of Ireland and the UK requesting proof of ID such as copy of a passport before processing the order. Any personal information supplied to us to validate an order is deleted or redacted within 72 hours.

1.1.3 Change of account information: Blacknight require proof of identity for a request to change the existing information on an account, such as changing an admin contact, change of ownership, change of company name etc. In such cases any information supplied to us is stored for period of 30 days in the event of a dispute arising within that time, and is then deleted automatically.

1.1.4 Ticketing Helpdesk: Blacknight utilise Zendesk, a cloud-based service provider for our helpdesk and ticketing system, and some personal information such as proof of ID can be submitted in response to a service request. Any personally identifiable information or credit card information submitted either on request or voluntarily is redacted by our staff as soon as is reasonably possible.

1.1.5 Livechat: Blacknight use Provide Support for the live-chat portal linked to our website. Transcripts of these "conversations" are recorded and offered to the customer on closing the session. A copy of the transcript is emailed to the Customer Experience Manager and retained for one year in the event a dispute arises regarding the conversation. We do not request or require any confidential information on this platform, other than an account ID related to the service being queried for validation purposes, and any other confidential or personal information provided will be at the Customers confirmation.

1.1.6 Telephone: Voice recordings are currently recorded and stored on an access-controlled server for a period of 30 days in the event of any dispute regarding what was said in a telephone conversation. The recordings are only accessible to the customer service manager and CTO.

1.2 Purpose Limitation

The collection of data at our control panel(s) enable online purchasing of our services and any security sensitive data such as credit card information is encrypted in accordance with our PCI compliance obligations. We collect personal data (This is data that identifies you or can be used to identify or contact you and may include your name, address, email address, telephone number and billing information. Such information is only collected from you if you voluntarily submit it to us.) We also collect non-personal data (information that cannot be used to identify or contact you, such as demographic information regarding, for example, user IP addresses where they have been clipped or anonymised, browser types and other anonymous statistical data involving the use of our website)
We do not share your personal information with Third Parties unless you have consented to it as required for the purpose of registering for any products we re-sell (such as SSL certs, Microsoft Office365, sitebuilder products and domain registrations) In those instances we currently have contractual agreements in place that ensure the 3rd party upholds it's GDPR obligations with regard to data security and privacy.

The data use is limited to

- Billing and account maintenance details
- Validation and accuracy of registration details
- Notifications relating to service outages or maintenance requirements
- Limited marketing activities and customer service follow up activities.

1.3 Data Minimisation & Data Retention

Blacknight maintain a policy of data minimisation to manage the data we control such as voice recordings, expired accounts, personal data submitted for the purpose of registration for a service, employee information, and we have a published Data Retention Policy for internal use indicating the maximum period for which we can retain certain types of data.
For Irish Revenue purposes we are required to retain all invoicing and billing records for a minimum period of 7 years after which time any soft or hard copies of that data are securely destroyed in accordance with our ISO framework.

1.4 Accuracy

Where feasible Blacknight will make every possible effort to ensure the data we hold relating to a data subject is kept up to date and accurate. We may do this by periodically contacting the data subject via email with requests that the data is verified by the data subject.
Blacknight reserve the right to suspend any services which were purchased under fraudulent pretense and forward any relevant data to An Garda Siochana.

1.5 Integrity and Confidentiality

The core tenets of ISO27001 are confidentiality, integrity and availability. Blacknight observe these core values and are regularly tested on them both externally and with internal audits. Blacknight's management regularly review and assess its exposure to Data Security risk and mitigation and operate a continuous improvement process with regard to protecting ourselves and our customers.

1.6 Accountability

Blacknight already implement appropriate technical and organisational measures as part of our ISO27001 framework and adhere to strict governance and /or codes of conduct guidelines from bodies such as ICANN, NCSC, PCI, ISPAI, Irish Data Protection Authority etc.