GDPR - Data Processing FAQ

2018

What is GDPR?

The General Data Protection Regulation (GDPR) is a new European data protection regulation adopted by the EU Commission. It replaces the EU Data Protection Directive, also known as Directive 95/46/EC. The GDPR becomes effective on May 25, 2018 and will strengthen security of and regulate personal data in the broadest sense. The GDPR applies to both individuals and businesses and regulates the way in which personal data of citizens in the European Union should be handled.

The following will be useful for customers wish to know our status with regard to their customer data and their own GDPR compliance.

When it comes to "Customer Data", is Hosting Ireland a controller or a processor?

Under GDPR, a "controller" determines why and how personal data is processed. A "processor" processes personal data on behalf of the controller. Hosting Ireland has limited knowledge of the data that each customer processes via the hosting infrastructure ("Customer Data"). Hosting Ireland only processes "Customer Data" in accordance with the customer's instructions. Therefore, Hosting Ireland is a processor of "Customer Data" hosted at Hosting Ireland; the customer is a controller and ultimately is responsible to the Data Protection Commissioner. Any content posted, uploaded, sent to or otherwise made available by you or your own data subjects on your hosting account is not subject to our Privacy Notice but is subject to our Terms and Conditions.

What have we done for GDPR?

- Appointed a Data Protection Officer
- We have documented all processing activities along with the lawful processing basis
- Conducted a Data Impact Assessment
- Conducted due diligence and obtained contracts for third-parties and sub-processors
- Updated policies including Privacy Policy, Privacy Impact Assessment Policy, Security Policies, Retentions Policy, Data Destruction Policy and Breach Reporting Procedures
- Conducted GDPR Staff Awareness Training
- Imposed additional confidentiality obligations on our Staff
- Updated our Terms & Conditions of Service which is our contract with customers
- Provided documentation about our services to help customers meet regulatory obligations.

Where is "Customer Data" held?

"Customer Data" is primarily stored in BT City West Datacentre, Dublin, Ireland (within the EU/EEA). Backups may also be stored in AWS Dublin, Ireland.

Other services may require transfer of data.

How do you protect "Customer Data"?

We have taken all reasonable steps (including appropriate technical and organisational measures) to protect "Customer Data". This would include physical, host level and network security.

In the case of Virtual and Dedicated servers the host and application level security is the responsibility of the client.

In the case of Shared Web Hosting the web site/application security is the responsibility of the client.

Who accesses the systems where the "Customer Data" is stored and how is this controlled?

Our technical support staff have limited knowledge of your "Customer Data". We will only access in connection to technical support, debugging, taking backups, malware scanning or other system administration tasks. Our staff have signed appropriate confidentiality agreements. All staff are based within the EU/EEA. Our IT Security Policy and sub policies detail the controls in-place to provide appropriate security.

Can you provide data portability for "Customer Data"?

Typically a customer will be able to access and migrate their "Customer Data" using secure file transfer protocols without assistance from us.

Do you have a process in place to inform the controller of any possible use of sub-processors that have access to "Customer Data"?

Yes, this outlined in our Terms and Conditions Addendum.

What is the policy for deletion of "Customer Data"?

This is outlined in our internal Retention Policy and Data Destruction Policy. In brief "Customer Data" will be removed 30-90 days after termination of services depending on product or service.

What is the policy when experiencing a data breach containing "Customer Data"?

This is detailed in our internal Data Breach Response and Notification Procedure. Depending on the product and access we have, we will:

- Notify the controller (customer) without undue delay
- Provide a description of the nature of the breach
- Provide details of measures taken to address the "customer data" breach
- Provide any information relating to the data breach
- Preserve available digital evidence for forensic needs

Do you have an assigned DPO within your organization who is properly involved, and notified in a timely manner with all issues which relate to the protection of personal data?

Yes, our Data Protection Officer can be contacted via dpo@hostingireland.ie

Is an Information Security Policy in place?

Yes, we have an Information Security Policy which oversees other policies including our IT Security Policy, Access Control Policy, Password Policy, Clear Desk/Screen Policy and Data Destruction Policy.

Do you have any Data Security Accreditation?

Yes, we have Cyber Essentials Certification. The BT Data Centre where "Customer data" is stored has ISO 27001, ISO 20000, ISO9001 and ISO14001 certification.

How is "Customer Data" secured?

We implement appropriate technical and organizational measures to secure "Customer Data" such as technologies including but not limited to Encryption, Network Monitoring, Malware Scanning,

Vulnerability Scanning, Network Security, Firewalls, Intrusion Detection/Protection, Access Control and Dual Factor Authentication. The responsibilities and methods used will depend on the exact service provided.

What features do you offer to help with GDPR?

We have a number of features you may wish to enable to help with your own GDPR compliance including:

- Website SSL Certificates
- TLS Encrypted Email Transport
- TLS Encrypted FTP Transport
- Client Area & Control Panel Two-Factor Authentication
- Spam Filtering
- Malware scanning (Automaticly Enabled)
- Patching of popular Web Application (Automaticly Enabled)

Do you invest in ongoing data protection security?

Yes, we promote a continuous improvement methodology by regularly testing the integrity and resilience of our systems and processes, making appropriate improvements where necessary.