# HST SOLUTIONS LIMITED

## GDPR Compliance

## Re: VPS hosting and Managed Services

With implementation of the General Data Protection Regulation 2016 ("**GDPR**") from 25th May 2018, customers are increasingly anxious to understand if they will be compliant with GDPR when utilizing virtual servers, dedicated server or managed web hosting services ("**Relevant Services**") of HST Solutions Limited ("HST").

Most of HST's customers of Relevant Services are Data Controllers, even if they do not hold personal data of their end users/clients/customers, they usually at least hold personal data of their employees. For the first time, the GDPR also puts statutory obligations on Data Processors, with effect that our customers who act as processors also have increased concerns about data security.

Regardless of which Relevant Service the customer utilizes, HST acknowledges that personal data is being stored by the customer on HST's equipment. As such there are obligations on both HST and our customer to ensure such data is kept safe.

This statement is broken into two main sections:

(i) an analysis of the obligations with regard to data security, and a summary of how HST meets those obligations,
(ii) an assessment on the specific Relevant Services and whether a Data Processing Agreement is required in each case.

### A. SECURITY OF DATA AND ITS PROCESSING

### (I) The Rules and requirements

The security of the data center is part of the security ecosystem that customers evaluate to determine whether the personal data they control or process is adequately protected.

Article 32 of the General Data Protection Regulation (GDPR) requires Data Controllers and Data Processors to implement "*appropriate technical and organizational measures*" that ensure a level of data security appropriate for the level of risk presented by processing personal data, and protect it from destruction, theft, loss, alteration or unauthorized disclosure.

GDPR Article 32 also (as outlined below) provides specific suggestions for what kinds of security actions might be considered "*appropriate to the risk*".

GDPR obligates controllers to engage only those processors that provide "*sufficient guarantees to implement appropriate technical and organizational measures*" to meet the GDPR requirements and protect data subjects' rights. For HST customers, it means that when acting as either a Data Controller or a Data Processor, and utilizing Relevant Services, they need to be comfortable that HST has the appropriate infrastructure and procedures to keep their data secure.

Controllers and processors that adhere to either an approved code of conduct or an approved certification mechanism (as described in Article 40 and Article 42) may use these tools to demonstrate compliance with the GDPR security standards.

**(II) How does HST comply?**

HST's uses Contabo (**"Datacenter Vendor"**) as their preferred data center supplier, Contabo's Technical and organizational measures for a) "Confidentiality", b) "Integrity", c) "Availability & Resilience" and d) "Procedures for regular testing, assessment & evaluation" are available at request, our datacenter provider is located in Germany.

Under GDPR, companies will have to notify data authorities within 72 hours after a breach of personal data has been discovered. HST ensures a consistent and effective approach to the management of information security incidents, including communication of security events.

In particular addressing the specific security actions set out in Article 32;

***(a) the pseudonymisation and encryption of personal data;***

In the context of the Relevant Services, HST does not have access to the personal data stored on behalf of customers. As such pseudonymisation and encryption of personal data is a matter for the customers when storing their personal data with HST's Relevant Services.

***(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;***

While HST provides the Virtual data center infrastructure and the security related to same, only the customers will have detailed knowledge of their applications, processing, types of data, categories of data subjects etc.

The VPS and managed cloud service or hosting is limited to providing Compute, Network and storage into which the customer installs its own software, and that software carries out the actual transactions with the data.

The customers are responsible for their own "logical security", firewalls, DDOS protection, authentications passwords etc. HST provides physical security via its preferred data center vendor Contabo as documented above.

The router through which customers access Relevant Services is separate from the HST internal corporate network, with centralized controls and restricted access internally.

***(c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;***

For Dedicated Servers or VPS, HST does not make or keep copies of the personal data, as such, in the unlikely event of a complete loss of the data center, the dedicated servers or VPS could be compromised for continuity of service.

While customers have taken precautions by locating the Personal Data at a certified Data Centre, some customers with particular concerns take the precaution of running parallel storage in a separate disaster recovery facility, or in a managed storage service.

***(d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.***

As part of its own GDPR compliance plan, HST has undertaken an analysis of is technical and organizational measures related to the security of data within its premises. HST runs regular staff training and updates with regard to data center security, and regular analysis of its data security processes.

**B. Specific Relevant Services and Data Processing Agreements.**

In principle, where a Data Controller uses the services of a Data Processor, it must have a written contract in place to govern the working relationship. These contracts must now include certain specific terms, as a minimum, designed to ensure that processing carried out by a processor meets all the requirements of the GDPR (not just those related to keeping personal data secure). HST have developed a standard Data Processing Agreement which is utilized where it provides Relevant Services and is deemed to be a Data Processor. A copy of that standard agreement is on the website www.HST.ie, and should be signed and returned to HST for countersignature.

**(I) COLOCATION**

HST sells colocation space in its supplier Data Centre, and provides associated power and security, and other facilities related services. When acting as a pure colocation operator, our position has been, and will remain, that HST is not a processor under GDPR. The hardware on which data is processed is not owned by HST, HST has no access to the data residing on the hardware, and HST provides no processing function in relation to it. Unless specifically ordered, we do not provide server relocation, patching or smart hands.

In those circumstances, HST does not believe a Data Processing Agreement is required, however we are aware there are differing views, and the risk exists that HST could become a processor as a result of an added service. HST is happy to sign a DPA if the Colocation customer requires it.

With regard to Colocation, there are some limited activities where HST as Colocation provider will process data. In terms of data centre security we, (i) require visitors to submit a passport or other identification to gain entry, and we record those details in order to maintain security, and (ii) CCTV over common areas of the Data Centre involves processing of data. HST is a controller of that data. Security Services are provided by a third party, and HST has a Data Processing Agreement with that security company, and the full force of the GDPR applies to that specific data e.g. mandatory record keeping, mandatory breach notification, detailed privacy notices in that context.

**(II) DEDICATED SERVERS**

Where HST provides a Dedicated Server service, it is possible, that although having no logical access to the data on the server, HST controls the physical security, and it often owns the server, so may act as Data Processor. The customer may require a DPA be signed between the customer and HST with regard to such personal data.