Viatel Ireland Limited:	GDPR Compliance: Storage, Colocation 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 utilising dedicated servers, colocation or managed storage services ("**Relevant Services**") of Viatel Ireland Limited ("**Viatel**").

Most of Viatel'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 utilises, Viatel acknowledges that personal data is being stored by the customer on Viatel's premises, or in some cases on Viatel's equipment. As such there are obligations on both Viatel 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 Viatel meets those obligations,
(ii) an assessment 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 centre 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 organisational 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 unauthorised 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 Viatel customers, it means that when acting as either a Data Controller or a Data Processor, and utilising Relevant Services, they need to be comfortable that Viatel 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 Viatel comply?

Viatel's state-of-the-art data centre has ISO27001 certification and operates to PCI DSS standards. Our data centre is located in Dublin 15 in a gated business park, with manned security at the gate entrance, CCTV, security patrols and pre-approved ID access. In addition to the adopted technical controls, structured documentation, monitoring, and continuous improvement, the implementation of ISO 27001 promotes a culture and awareness of security incidents in our organization. Our employees have the key skillsets and a level of awareness to be able to detect and report security incidents.

Under GDPR, companies will have to notify data authorities within 72 hours after a breach of personal data has been discovered. The implementation of ISO 27001 control A.16.1 (Management of information security incidents and improvements), 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, Viatel 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 Viatel's Relevant Services. Where a customer uses Viatel's managed storage service, the software allows the user to encrypt the stored data. This is a matter for the customer to select the encryption option on Viatel's managed storage interface.

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

Viatel believes that this requirement, in so far as it relates to the Colocation Services, is satisfied as set out above with ISO 27001 certification. For other Relevant Services, Viatel adheres to ISO 27001 standards, whether specifically certified or not for that particular service. While Viatel provides the physical data centre 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 colocation service is limited to providing a space, into which the customer installs its own equipment, and that equipment carries out the actual transactions with the data.

The customers are responsible for their own "logical security", firewalls, DDOS protection, authentications passwords etc. Viatel provides physical security.

The router through which customers access Relevant Services is separate from the Viatel internal corporate network, with centralised controls and restricted access internally. Viatel deploys industry standard firewalls and IT security systems to manage network security.

For the managed storage service, Viatel and the storage interface provider are responsible for logical security with regard to its interface with the customer's storage array. Customer is responsible for its own logical security. The customer deploys passwords and access rights on the storage service.

(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 Colocation, Viatel does not make or keep copies of the personal data, as such, in the unlikely event of a complete loss of the data centre, the colocation racks or dedicated servers 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.

Our managed storage solution offers a range of options to allow customers enhance their storage resilience, from mirroring options and parallel arrays to back-up managed storage at a separate location to the primary service. The customer can choose what levels of service it requires.

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

As part of its own GDPR compliance plan, Viatel has (in addition to its ISO certification), undertaken an analysis of is technical and organisational measures related to the security of data within its premises. Viatel runs regular staff training and updates with regard to data centre security, and regular analysis of its data security processes. As part of its ISO 27001 certification it also runs regular tests of disaster recovery scenarios.

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). Viatel have developed a standard Data Processing Agreement which is utilised where it provides Relevant Services and is deemed to be a Data Processor. A copy of that standard agreement is on the website www.viatel.com, and should be signed and returned to Viatel for countersignature.

(I) COLOCATION

Viatel sells colocation space in its 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 Viatel is not a processor under GDPR. The hardware on which data is processed is not owned by Viatel, Viatel has no access to the data residing on the hardware, and Viatel provides no processing function in relation to it. Unless specifically ordered, we do not provide server relocation, patching or smart hands.

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

With regard to Colocation, there are some limited activities where Viatel 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. Viatel is a controller of that data. Security Services are provided by a third party, and Viatel 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 Viatel provides a Dedicated Server service, it is possible, that although having no logical access to the data on the server, Viatel 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 Viatel with regard to such personal data.

(III) MANAGED STORAGE

Viatel acts as reseller of the Zadara managed storage product. For customers of that product, the personal data is physically kept on a server at the Viatel Data Centre, so the security and technical and organisational measures as outlined above apply equally. As regards processing, Viatel accepts that it is technically a processor, and that Zadara is a sub-processor of the personal data. Viatel also has a DPA with Zadara with regard to customer personal data that may be in the managed storage service.

Zadara's competence and compliance as sub-processor is itemised on its website. https://www.zadarastorage.com/compliance/.