NETBACKUP

NetBackup is a Customer-managed offering, where the Customer controls their information using either their own infrastructure or third-party hosting solution.

Where Customer does not utilize NetBackup as a Veritas managed cloud service, the Customer determines and controls NetBackup and its hosting configurations. In these instances, Veritas does not access or control any of the data. Therefore, Veritas would not be deemed a Data Processor.

Where Veritas manages NetBackup as a cloud service, Veritas would be deemed a Data Processor under Data Protection Legislation and the following provisions apply in accordance with the contract.

ANNEX 1

Data Exporter
The Data Exporter is (please specify briefly your activities relevant to the transfer):

Customer and those of its Affiliates that are permitted contractually to use the Veritas service known as NetBackup where Veritas manages such as a cloud service.

Data Importer
The Data Importer is (please specify briefly activities relevant to the transfer):

Veritas Technologies, LLC as the provider of the Service, where the Customer has contracted directly with the Data Importer, or as a subcontractor to Veritas Storage (Ireland) Limited.

Data Subjects
The Personal Data transferred concern the following categories of data subjects (please specify):

Any individual whose identifiable information may appear in Data Exporter's files.

Categories of Personal Data
The Personal Data transferred concern the following categories of data (please specify):

As determined by the Data Exporter, all categories of personal data may be processed. Common elements of personal data contained in the user files include but are not limited to, user names, file names, metadata and system logs and further identifiable information.

Special Categories of Personal Data
The Personal Data transferred concern the following special categories of data (please specify):

As determined by the Data Exporter all categories of personal data may be processed which includes any sensitive data contained within Data Exporter's files.

Processing Operations
The Personal Data transferred will be subject to the following basic processing activities (please specify)

The metadata are processed to enable the Data Exporter to back up and recover their data in various locations and across different storage configurations. The processing of Personal Data contained within the metadata is incidental to the purposes of the processing.

Sub-processors

To view a list of current sub-processors which may have access to Personal Data processed by the Service,

For information regarding any historical sub-processors related to your use of the Service, please contact privacy@veritas.com

ANNEX 2

SECURITY MEASURES

1. Access control to premises and facilities

Measures must be taken to prevent unauthorized physical access to premises and facilities holding personal data. Measures shall include:

- Access control system
- ID reader, magnetic card, chip card
- (Issue of) keys
- Door locking (electric door openers etc.)
- Surveillance facilities
- Alarm system, video/CCTV monitor
- Logging of facility exits/entries

2. Access control to systems

Measures must be taken to prevent unauthorized access to IT systems. These must include the following technical and organizational measures for user identification and authentication:

- Password procedures (incl. special characters, minimum length, forced change of password)
- No access for guest users or anonymous accounts
- Central management of system access
- Access to IT systems subject to approval from HR management and IT system administrators

3. Access control to data

Measures must be taken to prevent authorized users from accessing data beyond their authorized access rights and prevent the unauthorized (input, reading, copying, removal) modification or disclosure of data. These measures shall include:

- Differentiated access rights
- Access rights defined according to duties
- Automated log of user access via IT systems
- Measures to prevent the use of automated data-processing systems by unauthorized persons using data communication equipment

4. Disclosure control

Measures must be taken to prevent the unauthorized access, alteration or removal of data during transfer, and to ensure that all transfers are secure and are logged. These measures shall include:

- Compulsory use of a wholly-owned private network for all data transfers
- Encryption using a VPN for remote access, transport and communication of data.
- Prohibition of portable media
- Creating an audit trail of all data transfers

5. Input control

Measures must be put in place to ensure all data management and maintenance is logged, and an audit trail of whether data have been entered, changed or removed (deleted) and by whom must be maintained.

Measures should include:

- Logging user activities on IT systems
- Ensure that it is possible to verify and establish to which bodies personal data have been or may be transmitted or made available using data communication equipment
- Ensure that it is possible to verify and establish which personal data have been input into automated data-processing systems and when and by whom the data were input

6. Job control

Measures should be put in place to ensure that data is processed strictly in compliance with the data importer's instructions. These measures must include:

- Unambiguous wording of contractual instructions
- Monitoring of contract performance

7. Availability control

Measures should be put in place to ensure that data are protected against accidental destruction or loss.

These measures must include:

- Ensuring that installed systems may, in the case of interruption, be restored
- Ensure systems are functioning, and that faults are reported
- Ensure stored personal data cannot be corrupted by means of a malfunctioning of the system
- Uninterruptible power supply (UPS)
- Business Continuity procedures
- Remote storage
- Anti-virus/firewall systems

8. Segregation control

Measures should be put in place to allow data collected for different purposes to be processed separately.

These should include:

- Restriction of access to data stored for different purposes according to staff duties.
- Segregation of business IT systems
- Segregation of IT testing and production environments