DELL Technologies

Data Processing Schedule

This Data Processing Schedule ("**Schedule**") to the Agreement shall apply where the provision of services (the "**Services**") by Dell to you ("**Customer**") involves the processing of Personal Data which is subject to Privacy Laws and Dell acts as Processor on behalf of the Customer as the Controller. This Schedule does not apply where Dell is the Controller or where a third party acts as Processor on behalf of the Customer, under an alternative form of data processing agreement. In the event of conflict between this Schedule and the Agreement, this Schedule shall control with respect to its subject matter.

1. Definitions.

Terms not defined herein have the meanings set forth in the Agreement. The following words in this Schedule have the following meanings:

1.1 "**Agreement**" means the agreement between Customer and Dell for the provision of the Services to the Customer.

1.2 "**Controller**" means an entity which, alone or jointly with others, determines the purposes and means of the processing of the Personal Data.

1.3 "**GDPR**" means the General Data Protection Regulation (EU) 2016/679.

1.4 "**Model Clauses**" means, as applicable:

(i) the Standard Contractual Clauses for the transfer of personal data (Decision 2021/914/EU), as they may be amended or replaced from time to time, in respect of transfers from the European Economic Areas ("**EEA**") to third countries;

(ii) the International Data Transfer Addendum to the European Commission's Standard Contractual Clauses or the International Data Transfer Agreement, each as issued under Section 119A of the Data Protection Act 2018 in respect of transfers from the United Kingdom ("**UK**") to countries which are not subject to an adequacy decision under the UK GDPR; and/or

(iii) the Standard Contractual Clauses for the transfer of personal data (Decision 2021/914/EU), as they may be amended or replaced from time to time and as specifically amended for use under the Swiss Federal Data Protection Act by the amendments announced by the Swiss Federal Data Protection and Information Commissioner on 27 August 2021, in respect of transfers from Switzerland to third countries.

1.5 "**Personal Data**" means any information relating to an identified or identifiable natural person which is processed by Dell in the performance of the Agreement.

1.6 "**Personal Data Breach**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed under this Schedule.

1.7 "**Privacy Laws**" means any data protection and privacy laws to which a party to this Agreement is subject and which are applicable to the Services provided, including where applicable, GDPR, UK GDPR), the California Consumer Privacy Act ("**CCPA**") and other similar laws.

1.8 "**Processing**" means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

1.9 "**Processor**" means an entity which processes the Personal Data on behalf of the Controller.

1.10 "**Subprocessor**" means any Processor engaged by Dell for the provision of the Services.

1.11 "**UK GDPR**" means the GDPR as retained under UK domestic law further to the exit of the UK from the European Union, to be read alongside the UK Data Protection Act 2018, as may be amended from time to time.

2. Processing of Personal Data.

2.1 Roles of the Parties.

Dell may process Personal Data under the Agreement as a Processor acting on behalf of the Customer as the Controller.

2.2 Instructions.

Dell will process Personal Data in accordance with Customer's documented instructions. Customer agrees that this Schedule, the Agreement and any subsequent statements of work or services orders, and any configurations by Customer or its authorized users, comprise Customer's complete instructions to Dell regarding the Processing of Personal Data. Any additional or alternate instructions must be agreed between the parties in writing, including the costs (if any) associated with complying with such instructions. Dell is not responsible for determining if Customer's instructions are compliant with applicable law. However, if Dell is of the opinion that a Customer instruction infringes applicable Privacy Laws, Dell shall notify Customer as soon as reasonably practicable and shall not be required to comply with such infringing instruction.

2.3 Details of Processing.

Details of the subject matter of the Processing, its duration, nature and purpose, and the type of Personal Data and data subjects are as specified in Annex 2.

2.4 Compliance.

Customer and Dell agree to comply with their respective obligations under Privacy Laws applicable to the Personal Data that is Processed in connection with the Services. Customer has sole responsibility for complying with Privacy Laws regarding the lawfulness of the Processing of Personal Data prior to disclosing, transferring, or otherwise making available, any Personal Data to Dell.

3. Subprocessors.

3.1 Use of Subprocessors.

Dell may use Subprocessors with the Customer's general or specific written consent. Customer agrees that Dell may appoint and use Subprocessors to process the Personal Data in connection with the Services provided that Dell puts in place a contract in writing with each Subprocessor that imposes obligations that are: (i) relevant to the services to be provided by the Subprocessors and (ii) materially similar to the rights and/or obligations imposed on Dell

under this Schedule. Subprocessors may include third parties or any member of the Dell group of companies. Where a Subprocessor fails to fulfil its data protection obligations as specified above, Dell shall be liable to the Customer for the performance of the Subprocessor's obligations.

3.2 List of Subprocessors.

Dell will provide a list of Subprocessors that it engages to support the provision of the Services upon written request by the Customer or as otherwise made available by Dell on its website. Dell shall notify Customer of any changes to its list of Subprocessors. If Customer legitimately objects to the addition or removal of a Subprocessor on data protection grounds and Dell cannot reasonably accommodate Customer's objection, the parties will discuss Customer's concerns in good faith with a view to resolving the matter.

4. Security.

4.1 Technical and organisational security measures.

Taking into account industry standards, the costs of implementation, the nature, scope, context and purposes of the Processing, and any other relevant circumstances relating to the Processing of the Personal Data on Dell systems, Dell shall implement appropriate technical and organizational security measures to ensure security, confidentiality, integrity, availability and resilience of processing systems and services involved in the Processing of the Personal Data are commensurate with the risk in respect of such Personal Data. The parties agree that the technical and organisational security measures described in Annex 1 ("**Information Security Measures**") provide an appropriate level of security for the protection of Personal Data to meet the requirements of this clause. Dell will periodically (i) test and monitor the effectiveness of its safeguards, controls, systems and procedures and (ii) identify reasonably foreseeable internal and external risks to the security, confidentiality and integrity of the Personal Data, and ensure these risks are addressed.

4.2 Technical Progress.

The Information Security Measures are subject to technical progress and development and Dell may modify these provided that such modifications do not degrade the overall security of the Services provided under the Agreement.

4.3 Access.

Dell shall ensure that persons authorized to access the Personal Data (i) have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality and (ii) access the Personal Data only upon documented instructions from Dell, unless required to do so by applicable law.

5. Personal Data Breach.

Dell will notify the Customer without undue delay after becoming aware of a Personal Data Breach in relation to the Services provided by Dell under the Agreement and will use reasonable efforts to assist the Customer in mitigating, where possible, the adverse effects of any Personal Data Breach.

6. International Transfers.

Dell is authorized, in connection with the provision of the Services, or in the normal course of business, to make worldwide transfers of Personal Data to its affiliates and/or

Subprocessors. When making such transfers, Dell shall ensure appropriate protection is in place to safeguard the Personal Data transferred under or in connection with this Agreement. Where the provision of Services involves the transfer of Personal Data from the European Economic Areas ("EEA") or the UK or Switzerland to countries outside the EEA or the UK or Switzerland (which are not subject to an adequacy decision under Privacy Laws), Dell agrees it will use the applicable Model Clauses along with appropriate supplemental measures or other appropriate data transfer mechanisms in accordance with applicable Privacy Laws and, in particular, such transfers shall be subject to: (a) Dell having in place intra-group agreements with its affiliates which may have access to the Personal Data, which agreements shall incorporate the relevant Model Clauses and (b) Dell having in place agreements with its Subprocessors that incorporate the relevant Model Clauses as appropriate.

7. Deletion of Personal Data.

Upon termination of the Services (for any reason) and if requested by Customer in writing, Dell shall, as soon as reasonably practicable, return or delete the Personal Data on Dell systems unless applicable law requires storage of the Personal Data. Dell may defer the deletion of the Personal Data to the extent and for the duration that any Personal Data or copies thereof cannot reasonably and practically be expunged from Dell's systems. For such retention the provisions of this Schedule shall continue to apply to such Personal Data. Dell reserves the right to charge Customer for any reasonable costs and expenses incurred by Dell in deleting the Personal Data pursuant to this clause.

8. Cooperation.

8.1 Data Subject Requests.

Dell shall promptly inform Customer of any requests from individuals exercising their data subject rights under Privacy Laws. Customer is responsible for responding to such requests. Dell will reasonably assist Customer to respond to data subject requests to the extent that Customer is unable to access the relevant Personal Data in the use of the Services.

8.2 Third party requests.

If Dell receives any requests from third parties or an order of any court, tribunal, regulator or government agency with competent jurisdiction to which Dell is subject relating to the Processing of Personal Data under the Agreement, Dell will promptly redirect the request to the Customer. Dell will not respond to such requests without Customer's prior authorisation unless legally compelled to do so. Dell will, unless legally prohibited from doing so, inform the Customer in advance of making any disclosure of Personal Data and will reasonably co-operate with Customer to limit the scope of such disclosure to what is legally required.

8.3 Privacy Impact Assessment and Prior Consultation.

To the extent required by Privacy Laws, Dell shall provide reasonable assistance to Customer to carry out a data protection impact assessment in relation to the Processing of Personal Data undertaken by Dell and/or any required prior consultation(s) with supervisory authorities.

9. Demonstrating Compliance.

Dell shall, upon reasonable prior written request from Customer (such request to be made in accordance with the terms of the Agreement), provide to Customer such information as may be reasonably necessary to demonstrate compliance with Dell's obligations under this

Schedule and allow for and contribute to audits, including inspections, conducted by the Customer or another auditor mandated by Customer.

10. CCPA.

If Dell is Processing Personal Data within the scope of the CCPA, Dell will Process Personal Data on behalf of Customer and will not retain, use, share or disclose that Personal Data for any purpose other than for the purposes set out in this Schedule, the Agreement, and as permitted under the CCPA or any subsequent law. In no event will Dell share any Personal Data with third parties (except to Subprocessors providing the Services in accordance with clause 3 above) or sell any Personal Data. Each Party certifies that it understands and will comply with all restrictions placed on its' Processing of Personal Data, including by avoiding any action that would cause the other Party to be deemed to have sold Personal Data or Personal Information under the CCPA. For purposes of this paragraph, Processors hereunder will be considered Service Providers as defined in Section 1798.140 (v) of the CCPA.

Annex 1

Information Security Measures

Dell takes information security seriously. This information security overview applies to Dell's corporate controls for safeguarding personal data which is processed and transferred amongst Dell group companies. Dell's information security program enables the workforce to understand their responsibilities. Some customer solutions may have alternate safeguards outlined in the statement of work as agreed with each customer.

Security Practices

Dell has implemented corporate information security practices and standards that are designed to safeguard the Dell's corporate environment and to address: (1) information security; (2) system and asset management; (3) development; and (4) governance. These practices and standards are approved by the Dell CIO and undergo a formal review on an annual basis.

Organizational Security

It is the responsibility of the individuals across the organization to comply with these practices and standards. To facilitate the corporate adherence to these practices and standards, the function of information security provides:

1. Strategy and compliance with policies/standards and regulations, awareness and education, risk assessments and management, contract security requirements management, application and infrastructure consulting, assurance testing and drives the security direction of the company.
2. Security testing, design and implementation of security solutions to enable security controls adoption across the environment.
3. Security operations of implemented security solutions, the environment and assets, and manage incident response.
4. Forensic investigations with security operations, legal, data protection and human resources for investigations including eDiscovery and eForensics.

Asset Classification and Control

Dell's practice is to track and manage physical and logical assets. Examples of the assets that Dell IT might track include:

- Information Assets, such as identified databases, disaster recovery plans, business continuity plans, data classification, archived information.
- Software Assets, such as identified applications and system software.
- Physical Assets, such as identified servers, desktops/laptops, backup/archival tapes, printers and communications equipment.

The assets are classified based on business criticality to determine confidentiality requirements. Industry guidance for handling personal data provides the framework for technical, organizational and physical safeguards. These may include controls such as access management, encryption, logging and monitoring, and data destruction.

Personnel Security

As part of the employment process, employees undergo a screening process applicable per regional law. Dell's annual compliance training includes a requirement for employees to complete an online course and pass an assessment covering information security and data privacy. The security awareness program may also provide materials specific to certain job functions.

Physical and Environmental Security

Dell uses a number of technological and operational approaches in its physical security program in regards to risk mitigation. The security team works closely with each site to determine appropriate measures are in place and continually monitor any changes to the physical infrastructure, business, and known threats. It also monitors best practice measures used by others in the industry and

carefully selects approaches that meet both uniqueness's in business practice and expectations of Dell as a whole. Dell balances its approach towards security by considering elements of control that include architecture, operations, and systems.

Communications and Operations Management

The IT organization manages changes to the corporate infrastructure, systems and applications through a centralized change management program, which may include, testing, business impact analysis and management approval, where appropriate.

Incident response procedures exist for security and data protection incidents, which may include incident analysis, containment, response, remediation, reporting and the return to normal operations.

To protect against malicious use of assets and malicious software, additional controls may be implemented, based on risk. Such controls may include, but are not limited to, information security practices and standards; restricted access; designated development and test environments; virus detection on servers, desktops and notebooks; virus email attachment scanning; system compliance scans; intrusion prevention monitoring and response; logging and alerting on key events; information handling procedures based on data type, e-commerce application and network security; and system and application vulnerability scanning.

Access Controls

Access to corporate systems is restricted, based on procedures to ensure appropriate approvals. To reduce the risk of misuse, intentional or otherwise, access is provided based on segregation of duties and least privileges.

Remote access and wireless computing capabilities are restricted and require that both user and system safeguards are in place.

Specific event logs from key devices and systems are centrally collected and reported on an exceptions basis to enable incident response and forensic investigations.

System Development and Maintenance

Publicly released third party vulnerabilities are reviewed for applicability in the Dell environment. Based on risk to Dell's business and customers, there are pre-determined timeframes for remediation. In addition, vulnerability scanning and assessments are performed on new and key applications and the infrastructure based on risk. Code reviews and scanners are used in the development environment prior to production to proactively detect coding vulnerabilities based on risk. These processes enable proactive identification of vulnerabilities as well as compliance.

Compliance

The information security, legal, privacy and compliance departments work to identify regional laws and regulations applicable to Dell corporate. These requirements cover areas such as intellectual property of the company and our customers, software licenses, protection of employee and customer personal information, data protection and data handling procedures, trans-border data transmission, financial and operational procedures, regulatory export controls around technology, and forensic requirements.

Mechanisms such as the information security program, the executive privacy council, internal and external audits/assessments, internal and external legal counsel consultation, internal controls assessment, internal penetration testing and vulnerability assessments, contract management, security awareness, security consulting, policy exception reviews and risk management combine to drive compliance with these requirements.

Annex 2

Data Processing Description

1. Subject matter and duration of the Processing.

The subject matter and duration of the Processing shall be according to the Agreement.

2. Purpose of Processing.

Personal Data will be processed for the purpose of providing warranty- and support- related and/or deployment services, as relevant and defined by the selected service levels and support options. The Agreement and the relevant service descriptions and statements of work shall apply for the specifics and possible additional services.

3. Nature of Processing.

3.1 IT support.

Processor mainly processes IP-addresses, MAC-addresses or other technical IDs of IT-systems that are possibly assigned to a person. This generally happens, if necessary, by analyzing error-logs.

3.2 Support services.

Processor personnel may come into contact with Personal Data, contingent of Controller's internal policies, on the occasion of providing the customer and technical support services. This may happen by providing remote support or when entering Controller's premises to do hardware repair. In these occasions, the person incidentally may see documents, name tags, content on screens. The same may apply in cases of remote support screen sharing (e.g. via webex), if the Controller has not closed the relevant programs/software before the connection is established.

3.3 Trace dump files.

For certain products and in certain support situations a trace dump file may be analysed to assess the problem. A trace dump contains the read/write or transfer activity associated with an error. The content is generally written in OS error format and is agnostic to file types. Reconstruction of files and their potential content is not part of the analysis. It is highly unlikely that any personal information will be readable during the analysis.

3.4 Data storage devices.

Return or refurbishing of hardware storage devices (e.g. HDDs, SSDs, etc.), all data contained will be deleted or destroyed in automated processes.

4. Categories of Data Subjects.

The data subjects are Customer's end users, employees, contractors, suppliers and other third parties relevant to the Services.

5. Types of Personal Data.

The type of personal data that may be submitted by the customer are:

- Contact details: which may include name, address, email address, telephone, fax, other contact details, emergency contact details, associated local time zone information.

- Customer details: which may include contact details, invoicing and credit related data.
- IT systems and operational information: which may include personal identifiers, voice, video and data recordings, user ID and password details, computer name, email address, domain name, user names, passwords, IP address, permission data (according to job roles), account and delegate information for communication services, individual mailboxes and directories, chat communication data, software and hardware inventory, tracking information regarding patterns of software and internet usage (e.g. cookies), and information recorded for operational and/or training purposes).
- Data subjects' email content and traffic/transmission data; Online interactive and voice communications (such as blogs, chat, webcam and networking sessions); support services (incidental access may include accessing the content of email communications and data relating to the sending, routing and delivery of emails).
- Other: Any other Personal Data submitted by Customer to Provider as Customer's Processor.

6. Sub-processors.

6.1 The Processor may engage affiliated companies, subject to the requirements of the Data Processing Schedule, which include the conclusion of Model Clauses for relevant international transfers.

6.2 Additionally, third parties may be engaged, subject to the requirements of the Data Processing Schedule, which include the conclusion of Model Clauses for relevant international transfers.

Full details of Dell Subprocessors noted in sections 6.1 and 6.2 are set out at www.dell.com/subprocessors

7. Contact details of the Processor.

For data protection queries you can send a query to:

- The contact designated in the Agreement;
- Via an email to privacy@dell.com.