RELAX,
WE CARE

DATA PROCESSING ADDENDUM

IT-SUPPORT

Concluded between the „Parties“	
	NTS Netzwerk Telekom Service AG Parkring 4, 8074 Raaba-Grambach dataprivacy@nts.eu Fn173863g, LG f. ZRS Graz
„Controller“	**„Data Processor“**

1. PREAMBLE

1. Data Processor provides IT-Support and IT-Maintenance services on behalf of Controller on Controller's IT Infrastructure Systems. The extent of Data Processor's activities is outlined in the main (commercial) agreement between the Parties.
2. Since it is possible that Data Processor gains access to personal data during the IT-Support and IT-Maintenance activities or needs to process personal data to perform or be able to perform IT-Support and IT-Maintenance activities, Parties agree on enter into this Data Protection Agreement („DPA") according to Art 28 (3) GDPR.
3. Parties agree that in general neither party has an intention to perform content-related processing of personal data. In the event of accidental access to personal data are not seen as commissioned data processing.

2. SUBJECT

2.1. IT INFRASTRUCTURE SUPPORT

Processor will perform IT-Support and IT-Maintenance activities on Controller's IT Infrastructure Systems. In general Data Processor is not assigned with content-related processing of personal data. Commonly, the purpose of these activities is installation, operations support, and troubleshooting of IT Infrastructure Systems.

Data Processor's employees may gain access to personal data, or log-information or may be assigned with submission or deletion of such data.

In order to fulfill these assignments, Data Processor may access or transfer personal data (contact data, network traffic information, other personal data) from Controller's IT Infrastructure Systems.

Categories of affected persons are Controller's employees and Controller's customers.

2.2. MANAGED MONITOR

In case the controller is an active NTS Managed Monitor customer, Processor is appointed to collect technical data for monitoring purposes only. This data includes number of, type of and location of IT infrastructure systems. This includes backing up system configurations, collecting operational data from Controller's IT infrastructure systems. This data includes states of systems, MAC and IP addresses, traffic counters on interfaces, etc.

System configuration backups are performed as backup of technical configurations of the controller's IT infrastructure components and do not include databases of personal data. Processing of personal data is not the purpose of the Managed Monitor, nevertheless such data could be accessed unintentionally by Processor's employees.

As part of the appointment support or troubleshooting sessions might be performed, where personal data (e.g. IP or MAC addresses, names of IT equipment) is collected by Processors employees. This data is volatile and ephemeral and is never stored long-term and is never linked to other data by Processor.

Categories of affected persons are Controller's employees.

2.3. OTHER DATA AND SERVICES

It is Controller's sole responsibility to conclude a contract with their cloud service providers, if Controller has ordered cloud services (e.g. Meraki, Advanced Malware Protection, Umbrella, CWS, ...) through NTS. Although Processor might support Controller in configuring and maintaining the cloud service, a direct data processing agreement with the cloud operator is necessary concerning the data processed in the cloud.

3. PROCESSOR'S OBLIGATIONS

Processor shall:

1. only process personal data in accordance with applicable Data Protection Laws and as necessary to perform its obligations under this DPA and as instructed by the Controller (this may include any changes to applicable laws and necessary changes to Controller's internal guidelines and/or processes which may affect the Processor's Processing of personal data);
2. notify the Controller without undue delay, if it deems the Controller's instructions to be in violation of applicable Data Protection Laws.
3. inform the Controller as soon as reasonably possible of any enquiry, complaint, notice, request or other communication it receives from any supervisory authority, government, or any third party, relating to Processor's processing of personal data. Processor shall provide reasonable assistance to Controller to enable it to respond to such enquiries, complaints, notices, requests or other communications in line with applicable Data Protection Laws;
4. support the Controller by providing information and documents in response to any complaint, request or other communication made by a Data Subject, in particular in relation to the right to information, right of access, rectification, portability and right to object, to enable Controller to comply with those inquiries within the statutory periods set out in Data Protection Laws. Processor shall not communicate directly with any third party who requests disclosure of personal data unless obliged to do so by statutory law;
5. comply with its own obligations under applicable Data Protection Laws at all times including maintenance of records of processing (Records of Processing Activities), obtaining authorizations by Data Protection Authorities as applicable to the personal data;
6. provide assistance and any information needed by Controller to carry out a data protection impact assessment related to Processor's use of the personal data, to the extent the Controller does not otherwise have access to the relevant personal data.
7. notify the Data Controller without undue delay in writing to the agreed upon email address, if it has actual or constructive knowledge of the existence of any actual or suspected breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Company Data transmitted, stored, or otherwise processed (a "Data Breach").
8. in the event of a Data Breach in accordance with 7, Processor shall provide the Controller, without undue delay, and in any event within 72 hours following the actual or constructive knowledge of the Data Breach, with complete information related to the Data Breach, including but not limited to, the nature of the Data Breach, the nature of the Company Data affected, the categories and number of data subjects concerned, the categories and number of Company Data records concerned, the possible consequences of the Data Breach, the measures taken, or proposed to be taken, to address the Data Breach and mitigate its possible effects.
9. maintain a log of the Data Breach including facts, effects and remedial action taken. Furthermore, Processor shall take all steps to restore, reconstitute and/or reconstruct any personal data, which is lost, damaged, destroyed or corrupted as a result of a Data Breach as if they were Processor's own data, with all possible speed and shall provide Controller with all reasonable assistance in respect of any such Data Breach.
10. on the termination for whatever reason, or expiry of the DPA and/or Main Agreement, and where applicable at the choice of the Controller, destroy, or return in a format consistent with standard industry practices, all personal data and any copies thereof to the Controller. In case of returning of data, Processor is obliged to provide necessary support to Controller. If Controller elects for the Processor to destroy all the personal data, Processor shall certify to the Controller that it has done so, unless legislation imposed upon the Processor prevents it from destroying all or part of the personal data transferred. In any event, the Controller shall bear no costs for the Processor returning or destroying the personal data.

4. SUB PROCESSORS

1. Processor assigns sub-processors where necessary to fulfill maintenance obligations. This is limited to the Vendor or maintenance support partner (see Exhibit 2). Controller gives their explicit consent to this sub-assignment.
2. Processor shall procure, by written agreement, that all authorized sub-processors shall comply with the equivalent obligations applicable to Processor set out in this DPA. Processor shall upon Controller's request provide a copy of the written agreement concluded with the sub-processor.
3. Controller explicitly acknowledges and agrees to the assignment of additional sub processors that will comply with at least equivalent obligations applicable to Processor set out in this DPA. Additional sub processors will be assigned by Processor, if their services are essential for performing the obligations laid out in the main contract.
4. A list of all current sub processors is accessible at www.nts.eu/gdpr-subprocessors.
5. Controller may receive notifications of changes by sending an Email to subprocessors@nts.eu with the subject "Suscribe". Processor will then notify Controller of any change in the list of sub processors, before authorizing the sub processor.
6. Controller may reasonably object to the authorization of a new sub processor, if Controller has products or active maintenance contracts that have been built or sold by the new sub processor (i.e. is possibly affected by the new sub processor's services). This objection may only be raised because of

   6.1. reasonable concerns regarding data protection (e.g. if there are fact-founded reasons to expect data protection violations by the sub processor or non-sufficient technical and organizational measures by the sub processor)

   6.2. reasonable concerns regarding other violations of legal obligations by the sub processor

   6.3. other reasonable concerns founded in Controller's business interests or in data subject's interests (e.g. fact-based reasonable concerns about a potential disclosure of company data to competition or third parties)

   In case of an objection, Controller acknowledges that certain support- and maintenance activities might not be performed by Processor to the extent, they could be performed with the assistance of the objected sub processor.

5. TECHNICAL AND ORGANIZATIONAL MEASURES

1. Processor agrees to adopt necessary technical and organizational measures to ensure compliance with the applicable Data Protection Laws and with this DPA. An overview of measures implemented at the time of signing this DPA is set out in Exhibit 1.
2. Processor shall promptly inform Controller in writing about any material change to the technical and organizational measures.

6. AUDIT

1. Processor shall permit Controller, or a third-party auditor acting under Controller's direction, to conduct, data protection and/or security audits, assessments and inspections ("Audit") concerning Processor's data protection and security procedures relating to the processing of personal data, its compliance with this DPA and applicable Data Protection Laws. Controller may, in its sole discretion, require Processor to make available all information, access to premises, systems and staff in accordance with Processor's security regulations and data protection obligations (especially employee and other customer data).
2. 7.2 The Controller shall inform the Processor four weeks in advance about time and date of the Audit. Controller's right to conduct further audits in case Processor infringes data protection obligations remains unaffected.
3. Controller will bear all costs of the Audit.

7. CONFIDENTIALITY

1. Processor shall take all reasonable steps to ensure the reliability of any staff (including sub-processors) who may have access to, or are authorized to process, personal data and ensure such staff (including sub-processors) have committed themselves to appropriate obligations of confidentiality, or are under appropriate statutory obligations of confidentiality. Processor shall ensure that this obligation of confidentiality shall continue following the termination of any employment agreement, services agreement or this DPA.

8. TERMINATION

1. This DPA shall survive termination of the Main Agreement as long as Processor Processes personal data for the Controller. Following termination of the DPA, clause 7 shall remain in force.
2. To the extent that the Data Controller and the Data Processor have entered into additional agreements in conflict with this DPA, the provisions of this DPA shall prevail with regard to the processing of personal Data

9. GENERAL PROVISIONS

1. This DPA is governed by Austrian law, excluding its international private law (IPRG) and the UN-Convention on the international sale of goods (UN-Kaufrecht).
2. Parties irrevocably agree that the legal venue of this DPA is Graz and the responsible court for this legal venue has exclusive jurisdiction to settle any dispute arising out of or in connection with this DPA. Each Party agrees to waive any objection to the Governing Court, whether on the grounds of venue or that the forum is not appropriate.
3. In the event that individual provisions of this DPA are ineffective, the remaining provisions hereof continue in full force and effect.
4. Ancillary agreements must be made in writing. The foregoing shall also apply to the waiver of this mandatory written form.

Grambach 25th of May 2018

Controller	**NTS Netzwerk Telekom Service AG, as Processor**
Signature:	Signature
Name:	Name: DI Hermann Koller
Function	Function CFO

NETZWERK TELEKOM SERVICE AG

Parkring 4, 8074 Raaba-Grambach
T +43 316 405 455 – 0 F – 56
FN 173863g, Landesgericht f. ZRS Graz

10. ANNEX 1: TECHNICAL AND ORGANIZATIONAL MEASURES ("TOMS")

As an expert for IT-infrastructure, NTS has implemented comprehensive technical and organizational measures to protect employee and customer data. To ensure confidentiality, integrity and availability of Personal Data NTS has implemented periodical trainings of our staff and has successfully undergone an external certification according to ISO 27001.

1. CONFIDENTIALITY

Physical Access Control
Unauthorized access to systems, which process personal data, is not allowed. The relevant systems are protected by electronic key cards, keys and alarm systems, as well as super-vised by CCTV systems.

Logical Access Control
Unauthorized use of systems is not possible, because systems are protected by passwords. A clear password policy exists, which enforces the use complex passwords according to industry wide standards. The involved systems use password protected login-locks. Re-mote access to the NTS network is protected by two-factor authentication or similar technology.

According to valid security policies and procedures, supervised by ISO 27001 certification, it is not allowed to store customer data on client laptops permanently. Customer data is only stored on systems dedicated for this use. As an additional measure (defense in depth) all client laptops must use disk encryption.

Unauthorized reading, copying, change or destruction of data is not allowed on relevant systems. Specific access rights designed for a specific use of data must exist, prior to granting access. All access is logged.

Separation of Data Control
Data collected for a certain purpose are not merged or linked.

Transport
Unauthorized reading, copying or destruction of data is prevented during electronic transport of data. NTS provides platforms and systems which provide encryption on transport via public networks (e.g. secure transport to NTS file share platform). In addition, admin access to customer systems is encrypted with VPN (virtual private network) technology upon customer's request.

2. INTEGRITY

In case of electronic transmission of sensitive data encryption technologies (see chapter Transport above) can be used on customer's request. This is an effective countermeasure against unwanted alteration of data in transport.

Input Control
Access to relevant systems is controlled and change of data is logged.

3. AVAILABILITY AND RESILIENCE

NTS has ISO27.001 certified Business Continuity planning cycles in place, which are designed to improve data security on a regular basis. NTS uses anti-malware protection to minimize the risk of data loss.

4. PROCESS FOR REGULARY TESTING ASSESSING AND EVALUATING

NTS' ISO 27.001 certified Information System Management System (ISMS) ensures a valid Information Systems Security Policy. The whole ISMS is regularly reviewed and evaluated.
In addition, a Data Privacy Management System is established, which is regularly reviewed and evaluated.
Through these systems clear security roles and responsibilities are guaranteed. NTS regularly and voluntarily undergoes internal and external audits to recognize possible vulnerabilities in processes or systems. This enables NTS to be able to react promptly to such findings.
Incident handling processes ensure that threats are found fast and efficiently and are contained and eliminated as soon as possible.

ANNEX 2 – LIST OF SUBPROCESSORS

1. SISTER AND AFFILIATE COMPANIES

1. **NTS Netzwerk Telekom Service AG**, Parkring 4, 8074 Grambach, Austria
2. **NTS Deutschland GmbH**, Bahnhofplatz 3, 88045 Friedrichshafen, Germany
3. **NTS Italy, GmbH. – s.r.l.**, Schlachthofstraße, 30, 39100 Bozen, Italy
4. **NTS Schweiz GmbH**, Zinggenstraße 3, 9443 Widnau, Switzerland

   Transmissions in the context of technical support services based on the Commission Decision of the European Parliament and of the Council on the adequate protection of personal data provided in Switzerland 2000/518/EC.
5. **NTS Managed Service GmbH**, Parkring 4, 8074 Grambach, Austria
6. **NTS North America Corp.** Goldberg & Company, LLC 25B Vreeland Road, Suite 211. Florham Park, NJ 07932, USA

   Transmissions in the context of technical support services based on approved "Model Contract Clauses" (Commission Decision 2010/87/EU)

2. TECHNICAL SUPPORT PARTNERS

In case support of the following companies is needed to fulfill the subject of the contract, data (log files, remote sessions on customer systems)) is submitted or shown during support cases to countries outside the European Union. Where needed, data protection is given in countries outside the Union through legal instruments approved by the European Union.

2.1. PARTNER IN EUROPEAN UNION

1. **NTW Software GmbH**, Grabenweg 68, A-6020 Innsbruck

2.2. ENSURING OF DATA PROTECTION LEVELS BASED ON MODEL CONTRACT CLAUSES

Transmissions in the context of technical support services based on approved "Model Contract Clauses" (Commission Decision 2010/87/EU):

1. **Cisco Systems, Inc.**, 170 West Tasman Drive, San Jose, CA 95134, USA
2. **Citrix Systems, Inc.**, 851 Cypress Creek Road, Fort Lauderdale, FL 33309, USA
3. **NetApp, Inc.**, 1395 Crossman Ave, Sunnyvale, CA 94089, USA
4. **Dell EMC Inc.**, 176 South Street, Hopkinton, MA 01748, USA
5. **Palo Alto Networks Inc.**, 3000 Tannery Way, Santa Clara, CA 95054, USA

2.3. ENSURING OF DATA PROTECTION LEVELS BASED ON EU-US PRIVACY SHIELD

Transmissions in the context of technical support services based on „Privacy Shield" (Commission Decision (2016/1250/EU)

1. **Microsoft Corporation**, One Microsoft Way, Redmond, WA 98052-6399, USA
2. **Splunk Inc.,** 270 Brannan Street, San Francisco, CA 94107