Annex 1 to the MSA

PREAMBLE

This Annex specifies the data protection obligations of the parties which arise from commissioned data processing, as stipulated in the Agreement. It applies to all activities performed in connection with the Agreement in which the staff of the contract data processor on behalf ("Processor") or a third party acting on behalf of the Processor may come into contact with personal data of the Customer ("Controller").

1. DEFINITIONS

1.1. "Personal Data" means any individual element of information concerning the personal or material circumstances of an identified or identifiable individual.

1.2. "Processing" means commissioned processing of Personal Data, encompassing the storage, amendment, transfer, blocking or erasure of Personal Data by the Processor acting on behalf of the Controller.

1.3. "Instruction" means the written instruction, issued by Controller to Processor, and directing Processor to perform a specific action with regard to Personal Data (including, but not limited to, depersonalizing, blocking, deletion, making available). Instructions are specified in the Agreement (including Processor's Privacy Policy) and may, from time to time thereafter, be amended or replaced by Controller by separate written instructions (individual instructions).

2. SCOPE AND RESPONSIBILITY

2.1. Processor shall process the Personal Data listed in Exhibit 1 on behalf of Controller. Processing shall include such actions as may be specified in the Agreement. Within the scope of the Agreement, Controller shall be solely responsible for complying with the statutory requirements relating to data protection, in particular regarding the transfer of Personal Data to the Processor and the Processing of Personal Data (acting as "responsible body" as defined in section 3 (7) Federal Data Protection Act ("BDSG").

2.2. Based on such responsibility and subject to the relevant terms of the Agreement, Controller shall be entitled to demanding the rectification, deletion, blocking and making available of Personal Data during and after the term of the Agreement.

2.3. The regulations of this Annex shall equally apply if testing or maintenance of automatic processes or of Processing equipment is performed on behalf of Controller, and access to Personal Data in such context cannot be excluded.

3. OBLIGATIONS OF PROCESSOR

3.1. Processor shall collect, process and use Personal Data only within the scope of Controller's Instructions.

3.2. Within Processor's area of responsibility, Processor shall structure Processor's internal corporate organization to ensure compliance with the specific requirements of the protection of Personal Data. Processor shall take the technical and organizational measures listed in Exhibit 2 to protect Controller's Personal Data against misuse and loss in accordance with the requirements of the German Federal Data Protection Act (section 9 BDSG). Such measures hereunder shall include, but not be limited to,

3.2.1. Physical Access Controls designed to prevent unauthorized persons from gaining access to Personal Data Processing systems,

3.2.2. Logical Access Controls designed to prevent Personal Data Processing systems from being used without authorization,

3.2.3. Data Access Controls designed to limit persons entitled to use a Personal Data Processing system to only gain access to such Personal Data as they are entitled to access in accordance with their access rights, and that, in the course of processing or use and after storage, Personal Data cannot be read, copied, modified or deleted without authorization,

3.2.4. Data Transfer Controls designed to prevent Personal Data from being read, copied, modified or deleted without authorization during electronic transmission, transport or storage on storage media, and that the recipients for any transfer of Personal Data by means of data transmission facilities can be established and verified,

3.2.5. Entry Controls designed to create an audit trail to document whether and by whom data have been entered into, modified in, or removed from Personal Data Processing systems,

3.2.6. Instructions Controls designed to procure that Personal Data shall be Processed solely in accordance with the Instructions,

3.2.7. Availability Controls designed to protect Personal Data against accidental destruction or loss,

3.2.8. Separation Controls, designed to procure that Personal Data collected for different purposes will be processed separately.

A measure as referred to in Sections 3.2.2 - 3.2.4 shall be in particular, but shall not be limited to, the use of encryption technology; provided, however, that to the extent encryption is used, it shall be the responsibility of the Controller and not the Processor to determine whether and how to implement such encryption.

The specific technical and organizational measures are described in Exhibit 2.
3.3. Upon Controller's request, Processor shall provide all information necessary for compiling the overview defined by section 4 g para. 2 sentence 1 BDSG.
3.4. Processor has in place and shall maintain a process which requires that any personnel entrusted with Processing Controller's Personal Data have undertaken to comply with the principle of data secrecy in accordance with section 5 BDSG and have been duly instructed on the protective regulations of the BDSG. The secrecy undertaking shall continue after the termination of the above-entitled activities.
3.5. Processor shall provide to Controller the contact details of the Processor's data protection officer.
3.6. Processor shall, without undue delay, inform Controller in case of a serious interruption of operations, suspicion of breaches of Personal Data protection, and any other irregularity in Processing Controller's Personal Data.
3.7. Controller shall retain title as to any carrier media provided to Processor as well as any copies or reproductions thereof. Processor shall store such media in accordance with its service guides to protect it against unauthorized third party access. Upon Controller's request, Processor shall provide to Controller all information on Controller's Personal Data and information. Upon Controller's instruction, and subject to Controller procuring the relevant Services from Processor, Processor shall either hand over such material to Controller or store it on Controller's behalf.
3.8. Processor shall be obliged to audit and verify, or engage third parties to do so, the fulfilment of the above-mentioned obligations and shall maintain an adequate documentation of such verification.
4. OBLIGATIONS OF CONTROLLER AND PROCESSOR
4.1. Controller and Processor shall each comply with their own respective obligations under applicable data protection regulations.
4.2. Controller shall inform Processor without undue delay and comprehensively about any errors or irregularities related to statutory provisions on the Processing of Personal Data detected during an audit of the results of such Processing.
4.3. Controller shall maintain the publicly available register as defined in section 4 g para. 2 sentence 2 BDSG.
4.4. Controller shall be responsible for fulfilling the information obligations pursuant to section 42 a BDSG.
4.5. Controller shall, upon termination or expiration of the Agreement and by way of issuing an Instruction, stipulate the measures to return data carrier media or to delete stored data.
4.6. Any cost arising in connection with the return or deletion of Personal Data after the termination or expiration of the Agreement shall be borne by Controller.
4.7. Any cost arising out of Processor's performance under Instructions outside the Agreement's scope of work shall be borne by Controller.
5. ENQUIRIES BY DATA SUBJECTS TO CONTROLLER
5.1. Controller has instructed Processor in writing to do so, and
5.2. Controller reimburses Processor for the costs arising from this assistance.
6. AUDIT OBLIGATIONS
6.1. Prior to the commencement of Processing and in regular intervals thereafter, Controller shall have the right to audit the technical and organizational measures taken by Processor in accordance with the Agreement, and shall document the resulting findings.
For such purpose, Controller may
6.1.1.request information from Processor.
6.1.2.request that an expert's independent audit report is provided.
6.2. Processor shall, upon Company's written request and within a reasonable period of time, provide Controller with all information necessary for such audit. For the avoidance of doubt, Processor shall not be obligated to provide information regarding Processor's other clients.
7. SUBCONTRACTORS
7.1. Processor shall be entitled to subcontract Processor's data processing obligations defined in Section 2.1 that are dedicated solely to Controller to third parties only with Controller's written consent.
7.2. Controller acknowledges that Processor's contractual obligations hereunder, or the parts of the deliverables defined below, will be performed by the subcontractors listed in Exhibit 3, as such list may change over time.
7.3. Where Processor engages subcontractors to access Controller's Personal Data, Processor shall be obliged to pass on Processor's contractual obligations hereunder to such subcontractors. Sentence 1 shall apply in particular, but shall not be limited to, the contractual requirements for confidentiality, data protection and data security stipulated between the parties of the Agreement.
8. INFORMATION DUTIES
8.1. Where Controller's Personal Data becomes subject to search and seizure, an attachment order, confiscation during bankruptcy or insolvency proceedings, or similar events or measures by third parties while being Processed, Processor shall inform Controller without undue delay.

8.2. Processor shall, without undue delay, notify to all pertinent parties in such action, that any Personal Data affected thereby is in Controller's sole property and area of responsibility, that Personal Data is at Controller's sole disposition, and that Controller is the responsible body in the sense of the BDSG.	
CenturyLink Germany GmbH Name: Title: Date:	 Name: Title: Date:

EXHIBIT 1
A list of Personal Data elements and the purpose of their Processing by Processor on behalf of Controller. The list shall state the extent, the nature and purpose of any contemplated collection, processing and use of data, the type of data, and the circle of data subjects.

Service	**Public/Shared Cloud Service**
Type of Processor collected data	User information such as name, email address, title, office, phone number of Controller's employees or agents
Other data processed by Processor	Any information or data Controller stores, transmits, or processes using the Processor's services
Extent, type and purpose of the collection, processing or use of data.	Administration, management and support of the services provided to Controller.

EXHIBIT 2
Overview of the technical and organizational measures taken by Processor.
1. Access control
Measures to prevent unauthorized access to the data processing systems used to process personal data:
Physical access:
• Documented policies and procedures exist to help restrict and control access to the physical space
• Procedures exist and are followed to establish and make changes to the physical space
• Security personnel review valid government issued photo identification prior to allowing access to the facility
• New security personnel undergo a formal training program and their performance is report and reviewed monthly
• Dual control biometric readers and/or four digit personal identification numbers and or proxy cards are in place to help ensure that only authorized individuals have the ability to access the facility.
• Ingres man traps are in place and administered to help restrict access to the facility to only authorized individuals. Else, there needs to be continuous monitoring of facility access doors leading to the exterior.
• Internal and external monitoring of facility activity is performed through the use of 24x7 security guard personnel and security cameras.
• Biometric hand scan and/or proxy card access to the facility is electronically logged and maintained as per data privacy laws. Any exceptions or attempt of unauthorized access is tracked and escalated.
• Security guards perform a handover exercise upon change of shift.
Denial of use controls:
• Firewalls are used and configured to prevent unauthorized access. Firewalls are in place to control network traffic and prevent unauthorized traffic from passing between the internal network and external networks.
• A written policy addressing logical, physical security and availability has been approved by the Chief Security Officer and is implemented throughout the Company.
• A security policy and other policy documents have been developed to provide a framework to ensure the security and availability of the system.
• CenturyLink Cloud has a formal access control policy and account management procedures in place which detail the roles, responsibilities and process for adding, modifying and removing the accounts.
• Change management procedures are in place and have been reviewed and approved. These procedures include roles and responsibilities for change requests, approvals and execution.
• During yearly training sessions, security and availability policies are reviewed and discussed.
Job control:
• New employees and staff must sign a confidentiality and non-disclosure agreement as acknowledgement not to disclose proprietary or confidential information, including client information to unauthorized users.
• Employees are subjected to a criminal background check during the hiring process.
• Management assesses each job candidate to ascertain whether the candidate possess the requisite level of competence to fill the job position related qualifications and interview procedures.
• Employees undergo Security Awareness Training to educate them on the Policies and security. Refresher

training is held annually.
2. Controlled admittance
Measures and Processes that prevent unauthorized people from using the data processing systems and:
• CenturyLink Cloud has a formal access control policy and account management procedures in place which detail the roles, responsibilities and process for adding, modifying and removing the accounts.
• Access to systems is granted based upon specific department role and general corporate role assignments. Access rights are requested, approved, and documented via ticketing system per the Account Management Procedures.
• Network access employs user IDs and passwords unique to each users and user privilege restrictions mechanisms with privileges based on an individual's need to know.
• The ability to add or delete accounts and profiles is restricted to the Operations team and requires request and approval through the ticketing system.
• Only Operations personnel have access to backup data.
• Access to data centers is requested, approved, and documented via ticketing system per the account management procedures at each data provider.
3. Data Access control
Measures so that people authorized to use the data processing system can only access the personal data allowed by their access authorization.
• Access to data centers is requested, approved, and documented via ticketing system per the account management procedures at each data provider.
• Access to configure devices deemed sensitive is restricted to the Operations team and as per account management procedures
• Employees undergo Security Awareness Training to educate them on the Policies and security. Refresher training is held annually.
• External users are given the rights to control their Control Portal Account profile.
4. Data Transmission control
Measures so that unauthorized parties cannot read, copy, modify, or remove personal data during electronic transmission, or while the data is being transported or saved to a storage device, and that further guarantee that you can check and determine where personal data is to be transmitted using data transmission equipment.
• The Control Portal requires authentication through the web interface. It utilizes HTTPS as the encryption protocol.
• Virtual Private Networking (VPN) software is used to permit remote access by authorized users. Users are authenticated by the VPN server through specific "client" software and user ID and password.
5. Entry control
Measures so that you can later check and ascertain whether personal data has been entered, changed or modified in the data processing systems, and if so, by whom.
• Access to configure devices deemed sensitive is restricted to the Operations team and as per account

management procedures.
• Documented procedures exist for the collection, review, escalation and closure of system availability issues and potential security breaches.
• Anti-virus software is in place, including virus scans of incoming email messages. Virus definitions are updated daily.
• Network Active Directory policy ensures that passwords are at least seven characters in length, require complex characters, are changed every 72 days, and will lock out an account after 12 failed logon attempts.
6. Availability control
Measures so that personal data is protected against accidental destruction or loss.
• The production firewall system utilizes dual hardware devices configured in active/passive mode to ensure instantaneous failover in the event of hardware malfunction on the primary node.
• Changes are initiated, reviewed, and communicated to management and users through the Change Management Tools, as detailed in the change management procedures. These change requests include detailed implementation, test and rollback plans.
• Backup and restoration policies are documented and include the use of daily backups to local data center and to a remote data center.
• Management has created a disaster recovery policy to document the contingency procedures in place.
• Automated backup system are utilized to perform schedule system backups.
• Backup jobs are monitored and notification alerts are sent in the event of backup failures.
• Backups are performed in accordance with defined backup strategy and usability of backups is verified on a regular basis.
7. Separation control
Measures so that data collected for differing purposes can be processed separately.
• Passwords are required for logging into all applications and systems.
• Each customer service runs on its own private VLAN, and each virtual machine is isolated with zone-based firewalls. Customers can also use secure connections such as Persistent\User VPN, Direct Connection, or MPLS. •

Exhibit 3
List is Subcontractors instructed by Processor

- Equinix, colocation provider
- Amazon Web Services, object storage provider