

1. SCOPE, ORDER OF PRECEDENCE, AND TERM

- 1.1 This Schedule on U.S. Operations and U.S. Records is part of any master or standalone agreement between Contracting Entity and/or its Affiliates (collectively, “LLA”) and Supplier (the “Agreement”). Supplier enters into this Schedule on behalf of itself and its Affiliates. LLA and Supplier are individually a “party” and, collectively, the “parties.”
- 1.2 The effective date of the Schedule is the date of the Agreement, or the date that LLA first begins using the Services, whichever is earlier.
- 1.3 In the event of a conflict between this Schedule and the Agreement, this Schedule will control to the extent necessary to resolve the conflict.

2. DEFINITIONS

- 2.1 In this Schedule, the following terms shall have the following meanings:

“Access” means (1) to enter a location; and (2) to obtain, read, copy, edit, divert, release, affect, alter the state of, or otherwise view data or systems in any form, including through information technology (IT) systems, cloud computing platforms, networks, security systems, and equipment (software and hardware). For the avoidance of doubt, Access shall be construed broadly to include rather than exclude considered conduct.

“Contracting Entity” means the Liberty Latin America entity signatory to the Agreement.

“Domestic Communications (“DC”)” means wire communications, or electronic communications (whether stored or not) involving a PR/USVI Affiliate system, from one location within the United States, including its territories, to another location within the United States; or the U.S. portion of such wire communication or electronic communication (whether stored or not) that originates or terminates in the United States or its territories.

“Domestic Communications Infrastructure (“DCI”)” means any PR/USVI Affiliate system that supports any communications originating or terminating in the United States, including its territories, including any transmission, switching, bridging, and routing equipment, and any associated software (with the exception of commercial-off-the-shelf (“COTS”) software used for common business functions, e.g., Microsoft Office) used by, or on behalf of, PR/USVI Affiliate to provide, process, direct, control, supervise, or manage DC, but does not include the systems of entities for which PR/USVI Affiliate has a contracted arrangement for interconnection, peering, roaming, long-distance, or wholesale network access.

“Managed Network Service Provider (“MNSP”)” means any third party that has Access to Principal Equipment for the purpose of:

- (i) network operation; provisioning of Internet and telecommunications services; routine, corrective, and preventative maintenance, including switching, routing, and testing; network and service monitoring; network performance, optimization, and reporting; network audits, provisioning, creation and implementation of modifications or upgrades; or
- (ii) provision of DC or operation of DCI, including: customer support; Operations Support Systems (“OSS”); Business Support Systems (BSS); Network Operations Centers (“NOCs”); information technology; cloud operations/services; 5G (SDN, NFV, Applications); and datacenter services and operations.

“Personally Identifiable Information (“PII”)” means any information that uniquely identifies and correlates to a natural person or can be used to distinguish or trace a natural person’s identity alone, including, for example, his or her name, social security number, or biometric records, or, when combined with other personal or identifying information that is linked or linkable to a specific individual, including, for example, physical address, mobile number, email address, date and place of birth, or parent’s surname.

“Principal Equipment” means all telecommunications and information network equipment (including hardware, software, platforms, OS, applications, protocols) that supports telecommunications or information services, functions, or operations of a PR/USVI Affiliate.

“PR/USVI Affiliate” means a Liberty Latin America entity having systems and/or providing services in Puerto Rico and/or the U.S. Virgin Islands.

“Sensitive Data” has the meaning assigned in the Data Protection Agreement.

“Services” has the meaning given to it in the Agreement; otherwise, it means any services that Supplier provides to LLA under the Agreement.

“Supplier and Subcontractor Personnel” means all employees, agents, consultants and contractors of Supplier and/or of any Subcontractor.

“U.S. Records” means customer billing records, subscriber information, PII, call detail records, customer proprietary network information, and any other information (e.g. geo-location data, Sensitive Data, or information disclosing PII) used, processed (“processes” as used in this paragraph has the meaning assigned thereto in the Data Protection Agreement), or maintained in the ordinary course of business related to services offered or provided in the United States or its territories by a PR/USVI Affiliate.

3. SCOPE OF APPLICATION

3.1 This Schedule shall apply if Supplier provides any of the following to a PR/USVI Affiliate:

- (a) MNSP services;
- (b) NOC(s);
- (c) Network maintenance services;
- (d) Billing or customer support services;
- (e) Any operation or service that could potentially expose Domestic Communications, Domestic Communications Infrastructure or U.S. Records to unauthorized Access; and
- (f) Deploying any network elements, hardware, software, core network equipment, and network management capabilities.

4. NOTIFICATION OF SECURITY BREACHES

4.1 Supplier will report by email to dl-compliance@libertypr.com within 48 hours of becoming aware of any Security Breach involving U.S. Records, or any loss of U.S. Records, whether from a Security Breach, or other cause.

5. PERSONNEL SCREENING PROCEDURES

5.1 Supplier warrants it has in place screening processes for existing and newly hired Supplier and Subcontractor Personnel which includes background investigations, public criminal records checks, or other analogous means to ascertain a person’s trustworthiness.

6. NON-U.S. CITIZENS

6.1 If non-U.S. citizens will have Access to DC, DCI, Principal Equipment, or U.S. Records, Supplier must provide the following information to the United States government regarding each such non-U.S. citizen and must obtain approval from the United States government before providing Access to such non-U.S. citizen: full name; citizenship; date and place of birth; passport number and country; residence and business addresses, and phone numbers. PR/USVI Affiliate will provide Supplier with transmittal instructions.

- 6.2 Supplier must provide documentation of such approval for each non-U.S. citizen it seeks to provide Access to relevant records or systems. FAILURE TO OBTAIN SUCH APPROVAL WILL RESULT IN THE DENIAL OF SUCH PERSONS TO ACCESS THE RELEVANT RECORDS AND SYSTEMS. SUPPLIER CANNOT GRANT ACCESS TO DC,DCI, PRINCIPAL EQUIPMENT OR U.S. RECORDS PRIOR TO SECURING UNITED STATES GOVERNMENT APPROVAL.
- 6.3 Section 6.1 does not apply to incidental, non-recurring Access to DCI and Principal Equipment, including accompanying potential access to DC or U.S. Records, by non-U.S. citizens for software or equipment support and/or troubleshooting purposes.

7. NOTIFICATION OF SERVER LOCATION FOR U.S. RECORDS

- 7.1 Supplier will report by email to dl-compliance@libertypr.com the storage locations of U.S. Records and any changes to such locations 45 days in advance of making such changes. The PR/USVI Affiliate will make all the necessary efforts to obtain approval from the United States government before the change date. If government approval is not secured, the parties will discuss in good faith storage location alternatives. If no agreement is reached, this Agreement may be terminated with no penalties or further obligations to Supplier.

October 2022 version