

SCHEDULE

U.S. OPERATIONS AND U.S. RECORDS



1. DEFINITIONS

1.1 Unless expressed otherwise, all terms in the Schedule shall have the meanings set out in the Purchase Order Terms and Conditions.

1.2 In this U.S. Operations and U.S. Records 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.

"Call Detail Record" ("CDR") means the data records or call log records that contain information about each call made by a user and processed by switch, call manager, or call server.

"Contracting Entity" means the LLA entity signatory to the Agreement.

"Customer Proprietary Network Information" ("CPNI") means as set forth in 47 U.S.C. § 222(h)(1).

"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 a 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 date and place of birth, or parent's surname, or any "personal identifier information" as set forth in 31 C.F.R. § 800.502(c)(5)(vi)(B).

SCHEDULE

U.S. OPERATIONS AND U.S RECORDS



“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 an LLA entity having systems and/or providing services in or related to Puerto Rico, and/or the U.S. Virgin Islands.

“Security Breach” means a breach of security that caused or could cause an accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or Access to DC, DCI, or U.S. Records, or an event that qualifies as a reportable data breach under applicable data protection legislation.

“Sensitive Data” means the following types and categories of data: data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership; genetic data; biometric data; data concerning health, including protected health information governed by the Health Insurance Portability and Accountability Act; data concerning a natural person's sex life or sexual orientation; government identification numbers (e.g., SSNs, driver's license); payment card information; nonpublic personal information governed by the Gramm Leach Bliley Act, or analogous laws; an unencrypted identifier in combination with a password or other access code that would permit access to a data subject's account; and precise geolocation.

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

“Subscriber Information” means any information of the type referred to and accessible subject to the procedures set forth in 18 U.S.C. § 2703(c)(2) or 18 U.S.C. § 2709, as amended or superseded.

“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, CDRs, CPNI, and any other information (e.g., geo-location data, Sensitive Personal Data (as defined by 31 C.F.R. § 800.241), or information disclosing PII) used, processed, or maintained in the ordinary course of business related to the services offered or provided in the United States or its territories by a PR/USVI Affiliate, including information subject to disclosure to a U.S. federal or state governmental entity under the procedures set forth in 18 U.S.C. § 2703(c), (d) and 18 U.S.C. § 2709.

2. SCOPE OF APPLICATION

2.1 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 DC, DCI, or U.S. Records to unauthorized Access; and
- (f) Deploying any network elements, hardware, software, core network equipment, and network management capabilities.

SCHEDULE

U.S. OPERATIONS AND U.S. RECORDS



3. NOTIFICATION OF SECURITY BREACHES

- 3.1 In addition to any other obligations under the Agreement, Supplier will report by email to dl-compliance@libertypr.com within 48 hours of discovery of any Security Breach involving DC, DCI or U.S. Records, or any loss of U.S. Records, whether from a Security Breach, or other cause.

4. PERSONNEL AND ITS SCREENING PROCEDURES

- 4.1 In addition to any Supplier and Subcontractor Personnel provisions of the Agreement, Supplier shall:
- (a) Assume full responsibility of the management of all Supplier and Subcontractor Personnel. The acts and omissions of Supplier and Subcontractor Personnel shall be deemed to be those of Supplier; and
 - (b) Use the best endeavours to ensure continuity of Supplier and Subcontractor Personnel.
- 4.2 Subject to the restrictions and requirements of Section 5 of this Schedule, Supplier warrants, represents, and undertakes to LLA that:
- (a) it has in place screening processes for existing and newly hired Supplier and Subcontractor Personnel that includes background investigations, public criminal records checks, or other analogous means to ascertain a person's trustworthiness;
 - (b) Supplier and Subcontractor Personnel are adequately reliable, trained, skilled, experienced and qualified at a level appropriate to perform the functions ascribed to them; and,
 - (c) it shall provide LLA (a) with at least twenty-four (24) hours' prior written notice before replacing any Supplier and Subcontractor Personnel working in relation to the Services, or (b) notice within twenty-four (24) hours of notification that any Supplier Personnel ceases, for any reason (including resignation, termination, reassignment, suspension, or unavailability), to actively support the Services.
- 4.3 LLA may refuse access to, or remove from, any LLA premises any of the Supplier and Subcontractor Personnel. Upon LLA's reasonable written request, the Supplier and the Subcontractor shall, as promptly as is practical, subject to Section 5 of this Schedule, and at no additional cost, provide substitute Personnel.

5. NON-U.S. CITIZENS OR NATIONALS

- 5.1 If non-U.S. citizens or non-U.S. national will have Access to DC, DCI, Principal Equipment, or U.S. Records, Supplier must provide certain information in a format subject to LLA's instructions. This information may include, but is not limited to: full name and other names used; citizenship; date and place of birth; social security number; national ID; alien number; passport number and country; residence and business addresses, and phone number. LLA may require the Supplier to either submit to LLA, so that LLA may then submit to the U.S. government, or to submit directly to the U.S. government such information. All non-U.S. citizens or non-U.S. nationals must obtain approval from the U.S. government before requesting Access to DC, DCI, Principal Equipment, or U.S. Records and Access may not be requested until LLA has provided notice to Supplier of the U.S. government's approval.
- 5.2 FAILURE TO OBTAIN US. GOVERNMENT 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 U.S. GOVERNMENT APPROVAL.

SCHEDULE

U.S. OPERATIONS AND U.S RECORDS



- 5.3 Subject to consultation with LLA, Section 5.1 will 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.

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

- 6.1 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 U.S. government before the change date. If U.S. government approval is not secured, the parties will discuss in good faith storage location alternatives. If no agreement is reached, the Agreement may be terminated with no penalties or further obligations to Supplier.

October 2025 version