Safe Harbor Onward Transfer Schedule

This Safe Harbor Onward Transfer Schedule ("OTA Schedule") is subject to and incorporated by reference into the Agreement between Savvis Communications Corporation and its affiliates ("Savvis" or "Transferor") and the contractor ("Transferee Contractor" or "Transferee"). This OTA Schedule contains terms required of any contractor engaged by Savvis when Savvis transfers data that is subject to its Safe Harbor Certification

Transferee represents warrants and agrees that they will assume the data protection obligations pursuant to this OTA Schedule to the extent applicable to its activities for Savvis pursuant to its Safe Harbor Certification.

---

1. This OTA Schedule covers the access to or processing of personal data by \Transferee on behalf of itself and its customers regarding European Union data subjects in the course of providing services to Savvis.

2. Such personal data may include name, address, email address, date of birth, and telephone numbers.

3. The Transferee agrees to do all of the following regarding the transfer, processing, and use of such personal data in order to endeavor to protect it consistent with the relevant Safe Harbor Principles (a copy of which are attached hereto and incorporated herein):

a. Transferee and any other parties acting under its authority shall process the data only as directed by Transferor and contemplated by its obligations to to Transferor under the Agreement.

b. The Transferee shall enter into a contract with all subcontractors and other third parties having direct and material access to personal data that provides that they assume the same or similar data protection obligations as are incumbent upon the Transferee.

c. Transferee shall take the appropriate legal, organizational, and technical measures to protect the confidentiality of the personal data, including the precautions necessary to protect the personal data from loss, misuse, unauthorized access, disclosure, alteration and/or destruction, keeping in mind the nature of the personal data. In this context Transferee shall, upon request and within a reasonable time, correct, delete, and/or block personal data specifically identified by Transferor from further processing and/or use, and such actions may be subject to additional charges to Transferor as set forth in the Agreement provided Transferee provides Transferor notice of such changes in advance.

d. Transferee shall hold those of its employees or subcontractors with access to personal data accountable for violations of this OTA Schedule by imposing sanctions, which may include, where appropriate and subject to Transferee's discretion, the possibility of termination of contracts and employment.

e. Transferee shall process the personal data received from Transferor in accordance with the relevant Safe Harbor Principles.

f. Transferee shall designate a contact person within its organization authorized to respond to inquiries concerning processing of the personal data and will cooperate with Savvis concerning all such inquiries if so requested.

g. Transferee will submit its data processing facilities, data files and documentation needed for processing personal data to auditing and/or review by Savvis or its designated independent auditor to ascertain compliance with this OTA Schedule upon the request of Savvis, with reasonable notice and during normal business hours.

h. Transferee will notify Savvis of any provisions of local law (including any changes thereto), which do or could affect its ability to perform its obligations under this OTA Schedule.

4. Interpretation of this Agreement shall be governed by the laws of the State of Missouri without regard to its conflicts of law provisions.

5. Transferee shall indemnify and hold harmless Transferor and its successors and assigns (and their officers, directors, employees, sublicensees, customers, and agents) from and against any and all claims, losses, liabilities, damages, settlements, expenses, and costs (including, without limitation, attorneys' fees and court costs) that arise out of or relate to any breach (or claim or threat thereof that, if true, would be a breach) of this OTA Schedule by Transferee.

6. Termination.

a. This OTA Schedule shall remain in full force and effect for so long as the Agreement remains in effect, unless earlier terminated pursuant to Section 6(b) below.

b. Notwithstanding anything to the contrary, Savvis may terminate this OTA Schedule and the Agreement immediately, without judicial notice or resolution and

without prejudice to any other remedies, and without liability in the event of a breach by Transferee of any of its obligations under this OTA Schedule and Transferee fails to cure such breach within five (5) days; or (ii) Savvis determines that any processing by Transferee pursuant to this Agreement puts Savvis in breach, or threatened breach of its legal obligations; or (iii) Transferee assigns this OTA Schedule for any reason to a third party.

c. This OTA Schedule shall immediately terminate if the Agreement terminates for any reason.

d. Upon termination of this OTA Schedule for any reason, Transferee shall return all personal data, including copies to Savvis or at Savvis' request, shall destroy all copies of such personal data and certify to Savvis that you have done so.

SAFE HARBOR PRINCIPLES

- **NOTICE:** An organization must inform individuals about the purposes for which it collects and uses information about them, how to contact the organization with any inquiries or complaints, the types of third parties to which it discloses the information, and the choices and means the organization offers individuals for limiting its use and disclosure. This notice must be provided in clear and conspicuous language when individuals are first asked to provide personal information to the organization or as soon thereafter as is practicable, but in any event before the organization uses such information for a purpose other than that for which it was originally collected or processed by the transferring organization or discloses it for the first time to a third party.

- **CHOICE:** An organization must offer individuals the opportunity to choose (opt-out) whether their personal information is (a) to be disclosed to a third party or (b) to be used for a purpose that is incompatible with the purpose(s) for which it was originally collected or subsequently authorized by the individual. Individuals must be provided with clear and conspicuous, readily available, and affordable mechanisms to exercise choice. For sensitive information (*i.e.* personal information specifying medical or health conditions, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership or information specifying the sex life of the individual), they must be given affirmative or explicit (opt-in) choice if the information is to be disclosed to a third party or used for a purpose other than those for which it was originally collected or subsequently authorized by the individual through the exercise of opt-in choice. In any case, an organization should treat as sensitive any information received from a third party where the third party treats and identifies it as sensitive.

- **ONWARD TRANSFER:** To disclose information to a third party, organizations must apply the Notice and Choice Principles (except when disclosure is made to a third party that is acting as an agent to perform task(s) on behalf of and under the instructions of the organization). Where an organization wishes to transfer information to a third party that is acting as an agent, it may do so if it first either ascertains that the third party subscribes to the Principles or is subject to the Directive or another adequacy finding or enters into a written agreement with such third party requiring that the third party provide at least the same level of privacy protection as is required by the relevant Principles. If the organization complies with these requirements, it shall not be held responsible (unless the organization agrees otherwise) when a third party to which it transfers such information processes it in a way contrary to any restrictions or representations, unless the organization knew or should have known the third party would process it in such a contrary way and the organization has not taken reasonable steps to prevent or stop such processing.

- **SECURITY:** Organizations creating, maintaining, using, or disseminating personal information must take reasonable precautions to protect it from loss, misuse, unauthorized access, disclosure, alteration, and destruction.

- **DATA INTEGRITY:** Consistent with the Principles, personal information must be relevant for the purposes for which it is to be used. An organization may not process personal information in a way that is incompatible with the purposes for which it has been collected or subsequently authorized by the individual. To the extent necessary for those purposes, an organization should take reasonable steps to ensure that data is reliable for its intended use, accurate, complete, and current.

- **ACCESS:** Individuals must have access to personal information about them that an organization holds and be able to correct, amend**,** or delete that information where it is inaccurate, except where the burden or expense of providing access would be disproportionate to the risks to the individual's privacy in the case in question, or where the rights of persons other than the individual would be violated.

- **ENFORCEMENT:** Effective privacy protection must include mechanisms for assuring compliance with the Principles, recourse for individuals to whom the data relate affected by non-compliance with the Principles, and consequences for the organization when the Principles are not followed. At a minimum, such mechanisms must include (a) readily available and affordable independent recourse mechanisms by which each individual's complaints and disputes are investigated and resolved by reference to the Principles and damages awarded where the applicable law or private sector initiatives so provide; (b) follow-up procedures for verifying that the attestations and assertions businesses make about their privacy practices are true and that privacy practices have been implemented as presented; and (c) obligations to remedy problems arising out of failure to comply with the Principles by organizations announcing their adherence to them and consequences for such organizations. Sanctions must be sufficiently rigorous to ensure compliance by organizations.