**Transfer Impact Assessment**

**Destination Country: United States**

Data Importer:

* Four Winds Interactive LLC, 1221 Broadway Street, Denver CO 80203 USA; E-Search DAC, 5100 Cork Airport Business Park, Cork, T12 YE28, Ireland; Poppulo Inc., 77 4th Ave. Floor 6, Waltham, MA 02451 USA (collectively, “Poppulo”).
* Prepared By: Greenberg Traurig on behalf of Poppulo

Pursuant to Clause 14 of the EU Standard Contractual Clauses (SCCs) and the United Kingdom’s (UK) International Data Transfer Agreement (IDTA), the parties have agreed to document their assessment of the laws and practices in the above-referenced destination country. This document memorializes the parties’ understanding that Data Importer contractual obligations, combined with its internal procedures and security controls, are sufficient to protect European Economic Area (EEA) and United Kingdom (UK) personal data from the U.S. government’s mass surveillance and ensure that SCCs and will provide an acceptable legal transfer mechanism under the GDPR and UK GDPR.

| **Description of Relevant U.S. Laws & History of Governmental Access** | | |
| --- | --- | --- |
| **Law** | **Description** | **Data importer’s experience in last 5 years** |
| The Foreign Intelligence Surveillance Act of 1978 (FISA)  50 U.S.C. § 1801, et seq. (2021) | Pursuant to FISA, an independent court may authorize certain US government agencies (e.g., FBI) to issue orders for national security related purposes that require “electronic communications service providers” to disclose communications-related information of specific data subjects who are located outside of the US.  The term “electronic communications service providers” is defined to include “any service which provides to users thereof the abiltiy to send or receive wire or electronic communciations.” The term is widely understood in practice to apply to companies that are in the business of providing communications services to third parties (e.g., telecommunications carriers), as opposed to providing communcations services for internal corporate use such as employee email, although there is relatively little judicial interpretation of FISA’s scope. FISA, the ECPA (discussed below), and the Administrative Procedure Act authorize individuals of any nationality to seek redress in U.S. courts through civil lawsuits for violations of FISA 702. | None |
| Executive Order (EO) 12333 | EO 12333 refers to an executive order issued by the President of the United States organizing US intelligence activities. EO 12333 does not apply to the data importer as the order does not compel private companies, such as the data importer, to disclose personal data. Furthermore, EO 12333 does not directly authorize the government to require any company or person to disclose data, and on its own, does not permit bulk data collection. | None |
| Electronic Communications Privacy Act (ECPA) 50 U.S.C. § 1881(b)(4) (2021) | Pursuant to ECPA, the Federal Bureau of Investigation (FBI) may seek certain information relating to subscribers of “wire or electronic communication service providers.” The term “electronic communications service providers” is defined to include “any service which provides to users thereof the ability to send or receive wire or electronic communciations.” | None |
| CLOUD Act | Pursuant to the CLOUD Act, U.S. government agencies may seek any information from a communications service provider (“CSP”) who is subject to U.S. law, regardless of where the information is stored or located. The CLOUD Act also allows the executive branch to enter into bi-lateral agreements with foreign countries. These agreements eliminate conflicts of law issues, allowing CSPs to disclose electronic data directly to foreign authorities pursuant to covered orders without the use of a mutual legal assistance treaty. The CLOUD Act requires that all agreements with foreign territories include numerous provisions protecting privacy and civil liberties, and may only allow orders to be used to obtain information relating to the prevention, detection, investigation, or prosecution of serious crime, including terrorism. Among other things, all covered orders must be subject to review or oversight by an independent authority, such as a judge or magistrate | None |
| Executive Order 14086 on Enhancing Standard for United States Signals Intelligence Activities  (87 FR 62283)  (<https://www.federalregister.gov/documents/2022/10/14/2022-22531/enhancing-safeguards-for-united-states-signals-intelligence-activities> ) | This Executive Order (“EO”) establishes new principles and protections in relation to U.S. national security signals intelligence activities, and implements the commitments made by the U.S. in an agreement reached in principle on March 25, 2022 between President von der Leyen and President Biden. According to a press release issued by the European Commission, “the [EO] introduces new binding safeguards to address all the points raised by the Court of Justice of the EU [in the Schrems II decision of July 2020], limiting access to EU data by US intelligence services and establishing a Data Protection Review Court.” *See* <https://ec.europa.eu/commission/presscorner/detail/en/qanda_22_6045>. The EO requires that signals intelligence activities be necessary to advance a validated intelligence priority and shall be conducted only to the extent and in a manner that is proportionate to the validated intelligence priority for which they have been authorized. The EO also establishes a redress mechanism for complaints (submitted by an individual to their local data protection authority, which will then bring an action on their behalf in the U.S.). The initial investigation of complaints is performed by the Civil Liberties Protection Officer of the Office of the Director of National Intelligence (“ODNI CLPO”). The ODNI CLPO is authorized to investigate, review, and, as necessary, order appropriate remediation to ensure that signals intelligence activities comport with the EO. To do this, the ODNI CLPO will have access to all information necessary to make such a determination. In addition, the ODNI CLPO’s determination shall not be overseen or interfered with by the Director of National Intelligence. The ODNI CLPO’s orders are binding on each element of the Intelligence community, and they may only be reviewed by the Data Protection Review Court (established by the Attorney General’s regulation discussed below). As a result of this EO and the AG’s regulation, the European Commission has indicated that it “will now prepare a draft adequacy decision, as well as launch is adoption procedure.” See id. Following the adoption of a final adequacy decision, personal data will be able to flow freely and safely between the EU and U.S. companies certified by the U.S. Department of Commerce under the new EU-U.S. Data Privacy Framework. | Not applicable. |
| Attorney General Regulation Establishing the Data Protection Review Court  (28 CFR 201 et seq.)  (<https://www.justice.gov/opcl/page/file/1541321/download>) | Pursuant to the Executive Order on signals intelligence described immediately above, the Attorney General issued this rule to establish the Data Protection Review Court (“DPRC”) that will review the determinations concerning U.S. signals intelligence activities made by the ODNI CLPO. To ensure independence and impartiality, the DPRC judges will not be subject to day-to-day AG supervision and can only be removed for instances of misconduct, malfeasance, breach of security, neglect of duty, or incapacity. DPRC judgments, including remedial measures that the U.S. intelligence agencies must undertake, will be final and binding. To file for review, a data subject must file through their data protection authority within their country. Each complainant’s interests will be represented by a Special Advocate. Once DPRC review has been completed, data subjects will be informed if they did not uncover any violations or if they issued a determination requiring remedial measures. This regulation and the EO discussed above are likely to underpin a new adequacy decision for international data transfers to the U.S. from the EU. | Not applicable. |
| **Industry-level Knowledge**  *See* U.S. Privacy Safeguards Relevant to SCCs and Other EU Legal Bases for EU-U.S. Data Transfers after Schrems II (<https://www.commerce.gov/sites/default/files/2020-09/SCCsWhitePaperFORMATTEDFINAL508COMPLIANT.PDF>), dated September 2020, issued by U.S. Department of Commerce, U.S. Department of Justice and the Office of the Director of National Intelligence noting that:  U.S. government commitments and public policies restrict intelligence collection to what is required for foreign intelligence purposes and expressly prohibit the collection of information for the purpose of obtaining a commercial advantage. Companies whose EU operations involve ordinary commercial products or services, and whose EU-U.S. transfers of personal data involve ordinary commercial information like employee, customer, or sales records, would have no basis to believe U.S. intelligence agencies would seek to collect that data. Furthermore, the type of data that Data Importer processes on Data Exporter’s behalf is generally non-sensitive and of little interest to government authorities. | | |
| Administratively issued subpoenas or demands | Approximately 335 federal agencies have the ability to issue administrative subpoenas or civil investigatory demands compelling the production of documents or information. This includes, for example, the Securities Exchange Commission (SEC) and the Federal Trade Commission (FTC). In addition, agencies of the fifty states may have similar investigatory powers. Agencies generally **cannot** prohibit a company that receives an administrative subpoena or civil investigatory demand from disclosing that fact to a third party. | None |
| Search warrants | A search warrant is a court order that a judge issues to authorize a law enforcement officer to conduct a search of a person, office, or other location to identify, and confiscate, evidence of a crime. Agencies generally **cannot** prohibit a company that receives a search warrant from disclosing that fact to a third party. | None |
| Judicially issued subpoenas | A judicially issued subpoena is a formal written order issued by a judge that commands a person, or a company, to appear before a court, or to provide information to an officer of a court under penalty for failure to comply. Judges generally **cannot** prohibit a company that receives a judicial subpoena from disclosing that fact to a third party. | None |
| National Security Letters | A national security letter (NSL) is an administrative subpoena issued by the United States government (generally via the FBI) to gather information for national security purposes. NSLs do not require prior approval from a judge. The Stored Communications Act, Fair Credit Reporting Act, and Right to Financial Privacy Act authorize the United States government to seek such information that is "relevant" to authorized national security investigations. NSLs typically contain a nondisclosure requirement forbidding the recipient of an NSL from disclosing that a government agency has requested the information. As discussed in the context of FISA, while the Data Importer believes that it is not an electronic communication service provider, note that NSL’s might be indirectly relevant to the extent that data sent to the Data Importer through the internet or telephone may transit through a third party entity that is subject to a NSL-based government request. | None |

**Instructions to Data Exporter**: Please complete the risk assessment in the final column.

| **Circumstances of the Restricted Transfer and Factors Impacting Disclosure to Public Authorities** | | |
| --- | --- | --- |
| **Circumstances** | **Description** | **Impact on government access risk [to be completed by data exporter]** |
| 1. **Services Offered by Data Importer** | Data Importer provides a hybrid SaaS cloud solution with on-premise components facilitating omni-channel enterprise communications. | Choose an item. |
| 1. **Personal Data Transferred** | Data Exporter may submit Personal Data to Data Importer’s Services, the extent of which is determined and controlled by Data Exporter in its sole discretion, and which may include, but is not limited to the following categories of Personal Data:   * First and last name * Business contact information (company, email, phone, physical business address) * Personal contact information (email, cell phone) * Employment information (title, position, employer) * Communications information * ID data * Picture * Professional life data * Personal life data * Connection data * Localization data * For billing purposes, payment information   Pursuant to the agreement with Data Importer, Data Exporter is prohibited from submitting any sensitive data to the Services. | Choose an item. |
| 1. **Purpose of Processing** | Data Importer processes Personal Data to provide its omni-channel communications platform to the Data Exporter. | Choose an item. |
| 1. **Frequency of Transfers** | Continuous, for the duration of the Service agreement between Data Exporter and Data Importer | Choose an item. |
| 1. **Length of Processing Chain** | As a processor acting on behalf of Data Exporter, Data Importer can only process the personal information to provide its SaaS platform. To provide the Services, Data Importer may engage sub-processors in accordance with the Data Processing Agreement between the parties. A list of Data Importer’s sub-processors is available at: <https://poppulo.com/subprocessors>. | Choose an item. |
| 1. **Onward Transfers** | As a processor acting on behalf of Data Exporter, Data Importer can only process the personal information to provide its SaaS platform. To provide the Services, Data Importer may engage sub-processors in accordance with the Data Processing Agreement between the parties. A list of Data Importer’s sub-processors is available at: <https://poppulo.com/subprocessors>. | Choose an item. |
| 1. **Format of Transferred Data and How Data is Sent** | Data Importer employs encryption for data in transit and at rest. | Choose an item. |
| 1. **Technological and Organizational Security Measures** | Data Importer’s technical and organizational security measures are outlined in the Poppulo standard DPA. Poppulo maintains ISO 27001:2013 certification. These measures include:   * Adequate internal policies exist with clear allocation of responsibilities for data transfers, reporting channels and standard operating procedures for formal or informal requests to access the data (especially for intragroup transfers), including appointment of a specific team (IT, data protection and privacy experts) to deal with requests that involve personal data transferred from the EEA; notification to senior legal and corporate management and to the data exporter upon receipt of such requests; procedural steps to challenge disproportionate or unlawful requests; and provision of transparent information to data subjects. * Training for personnel in charge of managing requests for access, periodically updated to reflect new legal developments in the importing territory and EEA, including on EU requirements as to access by public authorities to personal data, in particular Article 52 (1) Charter of Fundamental Rights, raising awareness of personnel by assessment of practical examples of public authorities’ data access requests and by applying the Article 52(1) standard to the practical examples, taking into account data importer territory legislation and regulations applicable to the data importer (developed where possible in cooperation with the data exporter). * documenting and recording requests and responses provided to access requests (see Contractual measures above), including legal reasoning and actors involved (e.g. if the data exporter has been notified and its reply, the assessment of the team in charge of dealing with such requests, etc.); and these will be made available to the data exporter. * Implemented strict and granular data access and confidentiality policies and best practices, based on a strict need-to-know principle, monitored with regular audits and enforced through disciplinary measures, focusing on data minimisation with technical measures to restrict access (it might not be necessary to transfer certain data e.g. restricting remote access to EEA data for support, or when service provision only requires transfer of a limited dataset and not the entire database). * Implemented strict data security and data privacy policies, based on EU certification or codes of conducts or on international standards (e.g. ISO norms) and best practices (e.g. ENISA) with due regard to the state of the art, in accordance with the risk of the categories of data processed. * adopting and regularly reviewing internal policies to assess suitability of implemented complementary measures and identify and implement additional or alternative solutions when necessary, to ensure that an essentially equivalent level of protection is maintained. | Choose an item. |
| 1. **Data Retention** | Data Importer retains personal data for no longer than necessary to provide the Services to Data Exporter. Upon termination of the Services, data is returned and/or destroyed at the Data Exporter’s direction. | Choose an item. |
| 1. **Storage Location** | Personal information may be stored in any of the following locations: U.S.A., Ireland, U.K. | Choose an item. |
| 1. **Professional or Other Rules** | Data Importer is not subject to any professional or other rules, which apply in addition to the general legal regime of the United States. | Choose an item. |
| 1. **Economic Sector Involved** | Omni-channel communications software for employees and customers and space booking software | Choose an item. |

| **Additional Relevant Factors** | | | | |
| --- | --- | --- | --- | --- |
| **Circumstances** | **Description** | **If True Provide a Check (✓)** | **Impact on government access risk**  **[to be completed by data exporter]** |
| 1. **Comprehesive Data Protection Law** | While the U.S, does not have a comprehensive national data protection law, it has more then 300 federal and state laws governing the use, collection, sharing, and disclosure of personal data. | **✓** | Choose an item. |
| 1. **Independent Data Protection Authority** | The U.S. has several federal and state agencies with authority to enforce and monitor data privacy and data security practices including the Federal Trade Commission and California Privacy Protection Agency. | **✓** | Choose an item. |
| 1. **Interantioal Instruments / Treaties** | Data Importer is not aware of any international instruments or treaties to which the U.S. is subject in connection with data privacy or data security. | **✓** | Choose an item. |
| 1. **Availability of Judical Redress to Data Subjects** | Data subjects whose information is sought by a US government agency are generally permitted to seek redress in US courts. Note, however, that some US statutes identified above (e.g., FISA and ECPA) may prohibit a company that receives an information request from disclosing that fact. FISA, the ECPA, and the Administrative Procedure Act authorize individuals of any nationality to seek redress in U.S. courts through civil lawsuits for violations of FISA 702. However, with the establishment of the Data Protection Review Court, there is an additional redress mechanisms for EU data subjects who have been subject to signals intelligence by the U.S. government. | **✓** | Choose an item. |
| 1. **Law Enforcement Policy** | Data Importer has a policy and procedure in place for analyzing requests from law enforcement agencies. Among other things the Data Importer does not release client personal data to law enforcement unless it assesses that the demand is valid, and the release of client personal data is authorized or required by law. | **✓** | Choose an item. |

| **Contractual Safeguards Mandated by the IDTA Will Be Enforceable In the United States** | | | |
| --- | --- | --- | --- |
| **Factors suggesting there are enforceable rights and effective legal remedies** | **Description** | **If True Provide a Check (✓)** | **Impact on government access risk**  **[to be completed by data exporter]** |
| 1. **Recognition of the Rule of Law** | The U.S. recognizes the rule of law and has an established and respected legal and court system that is largely derived from the UK legal system. | **✓** | Choose an item. |
| 1. **Enforcement of Foreign Judgments** | Courts in the U.S. will recognize and enforce foreign judgments. The standard procedure is for the individual seeking to enforce the judgment to institute a new lawsuit before a competent U.S. court, which will then determine whether to recognize and enforce the foreign judgment and issue an appropriate order. | **✓** | Choose an item. |
| 1. **Judicial Independence** | Judicial process in the U.S. has a high level of integrity and the judicial system is respected as a separate and independent branch of the government. | **✓** | Choose an item. |

|  |  |
| --- | --- |
| **SUMMARY OF FINDINGS** | |
| Reviewer assessment | |
| Please provide your overall conclusion of the risk of this transfer: | [Insert reviewer assessment here - e.g. "In view of the assessments of the data importer, the data importer territory, the data transferred and the appropriate safeguards implemented by the data importer, the risk of proceeding with this transfer is [low/medium/high] risk."] |
| Please provide details of any risk mitigations measures recommended prior to transfer: | [E.g. any further necessary recommendations made by the reviewer for the transfer to proceed] |
| DPO assessment (if any) | |
| Please provide the DPO's overall conclusion of the risk of this transfer: | [Insert DPO assessment here - e.g. ""In view of the assessments of the data importer, the data importer territory, the data transferred and the appropriate safeguards implemented by the data importer, the risk of proceeding with this transfer is [low/medium/high] risk.]" |
| Please provide details of any risk mitigations measures recommended by the DPO prior to transfer: | [E.g. any further necessary recommendations made by the DPO for the transfer to proceed] |