Crownpeak Technology Inc.

Transfer Impact Assessment

This Transfer Impact Assessment ("TIA") discusses how Crownpeak Technology Inc. ("Crownpeak") uses sufficient supplementary safeguards, including the supplementary measures noted below in section 3 and the use of Standard Contractual Clauses (see the Data Processing Agreement), to proceed with the transfers of personal data. This TIA describes: the nature and purpose for data transfers; the third country of destination's laws and practices; supplementary safeguards applied to the transfer of data; and a conclusion on the remaining risk to a data subject.

1. **Nature and Purpose of the Data Transfer**
    a. The specific circumstances of the transfer can be found in Annex II of the DPA.
    b. Purpose of the Transfer:
    Performance of the Services pursuant to the Agreement.
    c. Categories of Transferred Personal Data:
    The following categories of customer data may be transferred to Crownpeak in a wide variety of formats (including spreadsheets, files, etc.), for processing:
        i. Personal data (authorized user's name, contact information, email address, pseudonymized data used to track users' consent choices, etc.)
        ii. Device identification data (IP address, location)
        iii. Any other personal data supplied by users

2. **Laws and Practices of the Third Country of Destination**
    a. Country of Destination: United States.
    The data processor (or sub-processor), Crownpeak is located in the United States ("US"). As of the date of this TIA, the US is considered to be a Third Country without an Adequacy Decision (as determined by the relevant authorities). The CJEU invalidated the Privacy Shield in July 2020, determining that US privacy laws do not have adequate limitations and safeguards in place on the basis that personal data may potentially be accessed by US law enforcement and national security agencies ("Schrems II judgment").
    At this time, Crownpeak has not been subject to a disclosure order under the Foreign Intelligence Surveillance Act 702 (codified 50 U.S.C. Section 1801, hereinafter "FISA") or Executive Order 12333 or otherwise been requested to disclose personal data of data subjects located in or subject to the applicable law of the European Economic Area, Switzerland, or the United Kingdom. Further, based on the type of customer data that Crownpeak processes and transfers, Crownpeak is not the type of entity likely to be subject to an order to disclose customer data under FISA 702 or EO 12333.
    In the unlikely event that we receive a request by the relevant authorities, Crownpeak will use all reasonably available legal mechanisms to challenge any demands for data access through national security process it receives as well as any non-disclosure provisions attached thereto.

3. **Supplementary contractual, technical or organizational safeguards.**
   While no risk of unwarranted disclosure to public authorities has been identified, Crownpeak has still implemented technical and organizational measures to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons in terms of its obligations as a data processor. These measures include encryption of data in transit and at rest and 24/7 system events logging.

4. **Conclusion.**
   The laws identified in the Schrems II judgment (FISA 702 and EO12333) find no application upon Crownpeak. As such, there is no risk of unwarranted disclosure to public authorities in the US and the consequent violation of data subject rights. Thus, there is no reason to believe that laws and practices of the country of destination prevent Crownpeak from fulfilling its obligations under the SCCs.