EU SCC Transfer Impact Assessment (TIA)

Last Updated January 12, 2023

This TIA applies to all Impartner modules other than News On Demand and Social On Demand

Section 1: Intended Transfer

a)	Data exporter:	Customer defined in Order Form
b)	Country of data exporter:	Country listed in Customer contact information in Order Form
c)	Data importer (or the recipient in case of a relevant onward transfer):	Impatner, Inc. 10619 South Jordan Gateway Suite 200, South Jordan, UT 84095
d)	Country of data importer:	U.S.A.
e)	Context and purpose of the transfer:	Importer provides its customers with a SaaS platform for the exporters to manage their partner relationship management (PRM) programs.
f)	Categories of data subjects concerned:	• Employees, agents, advisors, subcontractors or contact persons of Customer; • Customer's clients, channel partners, prospects, business partners, and vendors (who are natural persons); • Other authorized users of the Services.
g)	Categories of personal data transferred:	• Personal details, names, user names, passwords, email addresses of users • Personal data within emails which identifies or may be reasonably linked or linkable to an individual • Data Subjects' metadata including sent, to, from, date, time, subject which may be considered Personal Data • File attachments sent by Data Exporter or Data Exporter's partners which may contain Personal Data • Personal Data sent by users of their own accord in free text fields or in files uploaded • Personal Data Information offered by users as part of support enquiries • Technical operational data including without limitation IP addresses, logins, search queries; which may include Personal Data • Other data added by Exporter from time to time
h)	Sensitive personal data:	Importer's platform is not intended to process any sensitive personal data. Importer requests in its contracts with Exporters that such Exporters prohibit their employees from transmitting any sensitive personal data to Importer.
i)	Technical implementation of the transfer:	Importer's data centers are in the U.S.A. All data uploaded to Importer's platform, are transferred to said U.S. data centers via the Internet.
j)	Technical and organizational measures in place (optional):	Availabe at: https://impartner.com/wp-content/uploads/2022/11/Impartner-Technical-and-Organizational-Security-MeasuresQ4-2022-Web-Version.pdf
k)	Relevant onward transfer(s) of personal data (if any):	List of Sub-Processors Available at: https://impartner.com/wp-content/uploads/2022/12/Impartner-2022-12-01-List-of-SubProcessors.pdf
l)	Countries of recipients of relevant onward transfer(s):	U.S.A.

Section 2: Transfer Parameters

a)	Starting date of the transfer:	Upon execution of the licensing agreement with Importer
b)	Assessment period:	This assessment was performed on January 12, 2023, and shall remain effective until the earlier of (i) January 11, 2028, or (ii) the date upon which applicable law or facts require it to be re-assessed.
d)	Target jurisdiction for which the TIA is made:	U.S.A.

e)	Relevant local laws taken into consideration:	50 U.S.C. § 1881a (FISA 702); 47 U.S.C. § 153; 18 U.S.C. §§ 2510, 2711; EO 12.333; PPD-28	
Section 3: Safeguards			
a)	Would it be feasible, from a practical, technical and economical point of view, for the data exporter to transfer the personal data in question to a location in a whitelisted country instead?[7)]	No	Importer's 2023-2024 roadmap includes plans to establish data centers in the EU to isolate EU Personal Data processed by Importer so that such Personal Data will not need to be transferred outside of the EU. However, as of the Last Updated date listed above, such data centers are not ready to host data.
b)	Is the personal data transferred under one of the Art. 49 derogations?	No	The transfer is being made pursuant to the SCCs.
c)	Is the personal data at issue transmitted to the target jurisdiction in clear text (i.e. there is no appropriate encryption in-transit)?	No	All data in transit is encrypted using TLS 1.2 or higher
d)	Is the personal data at issue accessible in the target jurisdiction in clear text by the data importer/recipient or a third party (i.e. the data is either not appropriately encrypted or access to the keys to decrypt is possible)?	No	All data stored at rest is encrypted using AES256, but decryption may take place prior to access in some events.
e)	Is the personal data at issue protected by a transfer mechanism approved by the applicable data protection law?	Yes	SCCs