Raxar Technology Corporation
Privacy Policy

I. Overview

Raxar Technology Corporation ("Raxar") with the EU-U.S. Data Privacy program Framework (EU-U.S. DPF), the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. Data Privacy program Framework (Swiss-U.S. DPF) as set forth by the U.S. Department of Commerce. Raxar has certified to the U.S. Department of Commerce that it adheres to the EU-U.S. Data Privacy Framework program Principles (EU-U.S. DPF Principles) the UK Extension to the EU-U.S. DPF with regard to the processing of personal data received from the European Union and the UK (including Gibraltor) in reliance on the EU-U.S. DPF. Raxar has certified to the U.S. Department of Commerce that it adheres to the Swiss-U.S. Data Privacy Framework program Principles (Swiss-U.S. DPF Principles) with regard to the processing of personal data received from Switzerland in reliance on the Swiss-U.S. DPF. If there is any conflict between the terms in this privacy policy and the DPF Principles, the Principles shall govern. To learn more about the Data Privacy Framework (DPF) program, and to view our certification, please visit https://www.dataprivacyframework.gov/.

With respect to personal data received or transferred pursuant to the Data Privacy Frameworks, Raxar is subject to the regulatory and enforcement powers of the U.S. Federal Trade Commission.

II. Definitions

For the purposes of this Privacy Policy:

"Controller" means a person or organization which, alone or jointly with others, determines the purposes and means of the processing of Personal Data.

"Customer" means any entity that purchases the Service.

"Customer Data" means the electronic data uploaded into the Service by or for a Customer or its Users.

"EU" means the European Union and Iceland, Liechtenstein and Norway

"Personal Data" means any information, including Sensitive Data, that is (i) about an identified or identifiable individual and (ii) received by Raxar in the U.S. from the EU in connection with the Service.

“Processor” means any natural or legal person, public authority, agency or other body that processes Personal Data on behalf of a Controller.

“Data Privacy Framework Principles” means the Principles and Supplemental Principles of the Data Privacy Framework.

“Sensitive Data” means Personal Data specifying medical or health conditions, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, sex life, the commission or alleged commission of any offense, any proceedings for any offense committed or alleged to have been committed by the individual or the disposal of such proceedings, or the sentence of any court in such proceedings.

“User” means an individual authorized by Customer to access and use the Service.

III. Types of Personal Data Collected and Purpose

Raxar hosts and processes Personal Data to carry out functions and activities at the direction of and pursuant to the instructions of Raxar Customers or Users when they purchase our products, register with our website, log-in to their account, request information from us, or otherwise communicate with us. The types of Personal Data from Customers or Users Raxar may collect or have access to in connection with include:

- Name
- Email address
- Business address
- Business phone number
- Username
- Password
- Job title

In addition, data collection also occurs, for example, when a Customer visits Raxar’s website.

- Contact information, such as name, company, email address, and telephone number; and
- Personal Data in content Customers provide on Raxar’s website and other data collected automatically through the website (such as IP addresses, browser characteristics, device characteristics, operating system, language preferences, referring URLs, information on actions taken on our website, and dates and times of website visits).

Raxar may also obtain Personal Data, such as contact information, such as name, and financial account information, of its Customer’s representatives. Raxar uses this information to manage relationships with its Customers, process payments, expenses, and reimbursements, and carry out Raxar’s obligations under its contracts with Customers.

IV. Notice

Raxar notifies Customers and Users about its privacy practices, including the purposes for which it collects and uses Personal Data, the types of Personal Data Raxar collects, the types of third parties to which Raxar discloses the Personal Data and the purposes for doing so, the rights and choices

Customers and Users have for limiting the use and disclosure of their Personal Data, and how to contact Raxar about its practices concerning Personal Data.

V. Third Party Disclosures

Raxar discloses Personal Data only to Third Parties that include web hosting, payment processors, document collaboration services, and communication services who reasonably need to know such data. Such recipients must agree to abide by confidentiality obligations. All Third Parties receiving personal information must have a written confidentiality agreement in place between Customer and Third Party and Raxar and Third Party that meets or exceeds Data Privacy Framework standards.

Raxar may disclose Personal Data that our Customers and Users provide to our Service:

- To contractors, business partners, and service providers we use to support our Service;
- In the event Raxar sells or transfers all or a portion of its business or assets (including in the event of a merger, acquisition, joint venture, reorganization, dissolution or liquidation), in which case Personal Data held by us about our Customers will be among the assets transferred to the buyer or acquirer;
- If required to do so by law or legal process;
- In response to lawful requests from public authorities, including to meet national security, public interest or law enforcement requirements.

VI. Access

Customers and users in the EU, the UK, and Switzerland have the right to access their Personal Data. If such Personal Data is inaccurate or processed in violation of the Data Privacy Framework Principles, a Customer or User may also request that the Personal Data be corrected, amended, or deleted.

When Raxar receives Personal Data, it does so on its Customer's or User's behalf. To request access to, or correction, amendment or deletion of Personal Data, Customers or Users should contact Raxar that collected their Personal Data. Raxar will support such Customer or User as needed in responding to any request.

Pursuant to the Data Privacy Frameworks, EU, UK, and Swiss individuals have the right to obtain our confirmation of whether we maintain personal information relating to you in the United States. Upon request, we will provide you with access to the personal information that we hold about you. You may also may correct, amend, or delete the personal information we hold about you. An individual who seeks access, or who seeks to correct, amend, or delete inaccurate data transferred to the United States under Data Privacy Framework, should direct their query to privacy@raxar.com. If requested to remove data, we will respond within a reasonable timeframe.

VII. Choice

Raxar offers Customers and Users the opportunity to choose whether their Personal Data may be (a) disclosed to third-party Controllers or (b) used for a purpose that is materially different from the purposes for which the information was originally collected or subsequently authorized by the relevant Customers or Users. To the extent required by the Data Privacy Framework Principles, Raxar obtains opt-in consent for certain uses and disclosures of Sensitive Data. Unless Raxar offers Customers or Users an appropriate choice, the company uses Personal Data only for purposes that are materially the same as those indicated in this Policy. To exercise their choices, Customers and Users may contact Raxar as indicated in this Policy or the other Privacy Policies.

Raxar may disclose Employee Personal Data and Consumer Personal Data without offering an opportunity to opt out, and may be required to disclose the Personal Data, (c) to third-party Processors the company has retained to perform services on its behalf and pursuant to its instructions, (d) if it is required to do so by law or legal process, or (e) in response to lawful requests from public authorities, including to meet national security, public interest or law enforcement requirements. Raxar also reserves the right to transfer Personal Data in the event of an audit or if the company sells or transfers all or a portion of its business or assets (including in the event of a merger, acquisition, joint venture, reorganization, dissolution or liquidation).

We will provide an individual opt-out choice, or opt-in for sensitive data, before we share your data with third parties other than our agents, or before we use it for a purpose other than which it was originally collected or subsequently authorized. To request to limit the use and disclosure of your personal information, please submit a written request to privacy@raxar.com.

VIII. Liability for Onward Transfers

Raxar complies with the Data Privacy Framework's Principle regarding accountability for onward transfers. Raxar remains liable under the Principles if its onward transfer recipients process Personal Data in a manner inconsistent with the Principles, unless Raxar proves that it was not responsible for the event giving rise to the damage.

IX. Recourse

In compliance with the EU-US Data Privacy Framework Principles, Raxar commits to resolve complaints about your privacy and our collection or use of your personal information transferred to the United States pursuant to the DPF Principles. European Union, UK, and Swiss individuals with DPF inquiries or complaints should first contact at:

Address: Raxar
P.O. Box 320635
Tampa, FL 33679

Email address: privacy@raxar.com

Phone number: 877-710-0077

Raxar has further committed to refer unresolved privacy complaints under the DPF Principles to an independent dispute resolution mechanism, Data Privacy Framework Services, operated by BBB National Programs. If you do not receive timely acknowledgment of your complaint, or if your complaint is not satisfactorily addressed, please visit

https://bbbprograms.org/programs/all-programs/dpf-consumers/ProcessForConsumers for more information and to file a complaint. This service is provided free of charge to you.

If your DPF complaint cannot be resolved through the above channels, under certain conditions, you may invoke binding arbitration for some residual claims not resolved by other redress mechanisms. See https://www.dataprivacyframework.gov/s/article/G-Arbitration-Procedures-dpf?tabset-35584=2

X. Changes to this Policy

This Policy may be amended from time to time, consistent with the requirements of the EU-U.S. Data Privacy Framework principles. Appropriate public notice will be given concerning such amendments.

Effective Date: September 18, 2023