resolution economics LLC

PRIVACY SHIELD POLICY

Resolution Economics, LLC ("ResEcon") provides sophisticated economic, statistical and financial analyses, forensic investigations, dispute advisory, expert testimony, and specialized technology and analytic solutions to leading law firms, Fortune 500 companies and government agencies. We understand and appreciate that you trust ResEcon with respected information and we are committed to providing data privacy and security that empowers our Clients to manage, control and understand their own data and the policies overseeing its safekeeping and use.

I. Definitions

- "Controller" means a person or organization which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.
- "Data Subject" means an identified or identifiable individual. An identifiable individual is one who can be identified, directly or indirectly, by reference to Personal Data.
- "Department" or "DOC" means the U.S. Department of Commerce and, where applicable and necessary, may also mean the International Trade Administration ("ITA").
- "Personal Data" means information and data about an identified or identifiable individual that are within the scope of the Program, received by ResEcon in the United States from the European Union or Switzerland, and recorded in any form. Personal Data may include but is not limited to names, mailing addresses, e-mail addresses, identification numbers, IP addresses and other Sensitive Data.
- "Policy" means ResEcon's Privacy Shield Commitment as set forth in this document.
- "Principles" means the foundational commitments that a participant in the Program must adhere to in order to be compliant, see Principles section below.
- "Processing" means any operation or set of operations which is performed upon personal data, whether or not by automated means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure or dissemination, and erasure or destruction.
- "Program" means both the EU-U.S. and the Swiss-U.S. Privacy Shield frameworks as designed by the DOC, the European Commission and Swiss Administration, and as administered by the ITA.
- "Sensitive Data" means data that contains any of the following: racial or ethnic origin; political affiliation; religious or philosophical beliefs; trade union membership; data concerning health or sex life and sexual orientation; genetic data; and biometric data where processed to uniquely identify a person.

II. Principles

From time to time, ResEcon may collect, process and/or maintain Personal Data during the course of providing professional services to, and at the direction of, our Clients. Accordingly, ResEcon complies with the EU-U.S. and Swiss-U.S. Privacy Shield frameworks, respectively, to ensure adequate protections for Personal Data transferred from European Union ("EU") member countries, and Switzerland, and received in the United States ("U.S.") by ResEcon in reliance on this Policy and the Program. All ResEcon employees and agents that have access to Personal Data contemplated by this Policy are

responsible for conducting themselves in accordance with this Policy and the Program's Principles. If any conflicts should arise between this Policy and the Program's Principles, the Program's Principles shall govern. Program information and ResEcon's participation listing are available via: https://www.privacyshield.gov/

1. Notice. ResEcon is an active participant in the Privacy Shield framework and, as such, may collect, process and/or maintain Personal Data during the course of providing professional services to our Clients and may do so without the knowledge of Data Subjects.

    1.1 All ResEcon services contemplated by this Policy are executed at the direction of our Clients and we inform our Clients of the purposes for which services are provided.

    1.2 Our Clients therefore bear the responsibility and shall inform Data Subjects of the individual's rights under this Policy and the Principles.

2. Choice. In the event Personal Data is to be disclosed to a non-agent third party or where Personal Data is to be utilized for a purpose that is materially different from that for which it was initially collected or subsequently authorized, ResEcon, through our Client, shall provide Data Subjects with the opportunity to limit the use or disclosure, if a limited option is available, or opt out of such use or disclosure altogether.

    2.1 In the event that Sensitive Data is contemplated within the meaning of this clause, ResEcon, through our Client, shall require explicit Data Subject consent before proceeding.

3. Onward Transfer. In the event that ResEcon transfers Personal Data to a third party Controller, ResEcon shall contractually require that the third party Controller a) only Process such data for the limited and specified purposes; b) provide at least the same level of privacy protection as required by the Program; c) notify ResEcon if and when the Controller can no longer meet its obligation; and d) cease Processing and remediate any unauthorized Processing as necessary if unable to satisfy its obligations under the Program.

    3.1 ResEcon shall take reasonable and appropriate steps to ensure that the Controller effectively processes the transferred Personal Data in a manner consistent with the Program, and shall provide the Department of Commerce with relevant privacy provisions of its contract with the Controller as requested.

    3.2 ResEcon is liable within the parameters of the Program where an agent processes Personal Data in a manner inconsistent with the Principles, except where ResEcon is not responsible for the event giving rise to the damage.

    3.3 ResEcon may be required to disclose Personal Data in response to lawful requests by public authorities to the extent required to meet legal, regulatory, governmental, national security or law enforcement requirements.

4. Security. ResEcon shall take reasonable and appropriate measures to protect Personal Data covered by this Policy and the Program from loss, misuse and unauthorized access, disclosure, alteration and destruction, taking into due account the risks involved in the processing and the nature of the Personal Data.

5. Data Integrity & Purpose Limitation. ResEcon limits the Processing of Personal Data to information that is relevant for the intended and specific purpose, and ResEcon only maintains Personal Data for so long as required to satisfy and support the originally intended purpose.

    5.1 We protect Personal Data in all of the following manners: a) all data, including Personal Data, is transferred via encrypted methods; b) Personal Data is never utilized to key files

in databases; c) access to physical media and servers is restricted to necessary personnel; and d) deletion is executed with a defensible and irretrievable process.

    5.2   At the direction of the Client, we may use objective Processing functionality to execute many of the following culling techniques to further protect Personal Data: a) removing files containing extracted Personal Data; b) excluding files containing extracted Personal Data from use; and c) proactively redacting Personal Data from reviewable files as necessary.

    5.3   In limited cases and only in accordance with the Program, ResEcon may Process Personal Data for longer periods than originally intended or necessary for the time and to the extent such Processing reasonably services the purposes of archiving in the public interest, journalism, literature and art, scientific or historical research, and statistical analysis.

6.   <u>Access</u>. ResEcon respects and supports your right to know what Personal Data has been Processed by our firm at the direction of our Client and we appreciate that you may require access for purposes such as but not limited to the need to ensure Personal Data's accuracy and relevance for the purpose for which it was Processed. Accordingly:

    6.1   Data Subjects contemplated by the Program and this Policy may request to review their own Personal Data as Processed by ResEcon.

    6.2   Requests may be excepted in situations, but not limited to, where the burden or expense of providing access would be disproportionate to the risks to the Data Subject's privacy in the case in question, or where the rights of other Data Subjects would be violated.

    6.3   Approved Data Subjects may review their own Personal Data in accordance with applicable contractual requirements, this Policy and the Program.

    6.4   In the event you are allowed and required by the Program to correct, amend or delete certain Personal Data that is inaccurate or has been processed in violation of the Principles, you may do so only with truthful, complete and accurate information.

7.   <u>Recourse, Enforcement & Liability</u>. In compliance with the EU-U.S. and Swiss-U.S. Privacy Shield framework, ResEcon is committed to amicably resolving privacy complaints made directly to ResEcon and we shall respond to inquiries filed directly with ResEcon within 45 days from receipt. Please address direct inquiries to the following: privacy@resecon.com

    7.1   In the event that we are unable to resolve a complaint from an EU or Swiss citizen, we shall, at no cost to you, refer the unresolved matter to the International Centre for Dispute Resolution ("ICDR") of the American Arbitration Association ("AAA"). EU or Swiss individuals may also file a complaint directly with the ICDR/AAA via: http://go.adr.org/privacyshield.html

    7.2   For those matters that remain unresolved, the Program allows Data Subjects contemplated by this Policy and the Program to pursue prompt, independent and fair resolution through binding arbitration with the Privacy Shield Panel.

The Federal Trade Commission ("FTC") has committed to enforcement of the Program as it relates to ResEcon's participation, and will work together with EU privacy authorities to protect Personal Data. ResEcon may, from time to time, change or update this Policy to ensure continuing compliance with the Program, its enforcement and other applicable laws. This Policy was last updated on 9 August 2017.