LEWIS RICE LLC

E.U. AND SWISS EMPLOYEE DATA PRIVACY POLICY

I. INTRODUCTION

Lewis Rice LLC (the "***Firm***") provides this E.U. and Swiss Employee Data Privacy Policy (this "***Policy***") to explain our practices regarding the collection, use, and other processing of information information that identifies or could be used to identify a client's employee who resides in the European Union ("***E.U.***") (including the United Kingdom ("***U.K.***")) and Switzerland ("***Employee Data***") as described in more detail below. The Firm does not have direct employees who reside in the E.U. or Switzerland. We would only receive information from any clients of the Firm.

II. SCOPE

The Firm is committed to respecting and protecting personal information collected, maintained or otherwise processed by the Firm in the scope of its performance of legal services for its clients. In furtherance of the Firm's commitment, the Firm has certified to adhere to the Privacy Shield Principles (as defined below) regarding personal information related to employees of our clients residing in the European Union or Switzerland and processed in the scope of its performance of legal services for its clients.

III. CATEGORIES OF EMPLOYEE DATA

As used in this Policy, the term "***employee***" refers to an individual who resides in the E.U. (including the U.K.) or Switzerland and who is on the payroll, regardless of work schedule, number of hours worked or eligibility for benefits, of one of the Firm's clients. The term "***employee***" includes individuals who work full-time, part-time, variable (short-term) and seasonal schedules, as well as interns and individuals on inactive status such as a maternity or disability leave.

The Firm collects and processes the following categories of Employee Data:

- **General Employee Data:** name and contact information (home address, personal e-mail, personal phone number, photographs and emergency contact information), date of birth, government identification numbers, citizenship/residency, personal status (marital status, dependents), and other data collection permitted or required by applicable law related to an Employee.
- **Employee status:** full-time, part-time, active, leave of absence, and employment termination data.
- **Organization information:** work contact information, title, department, employer, cost center, location, hire date and any previous hire or service dates, supervisor, and job function.
- **Compensation information:** current base salary and differentials, annual salary, pay scale and range, type of employee, average hours worked, incentive information, equity and other compensation program participation, and salary history.
- **Payroll information:** bank information, tax information, garnishments and deductions, time worked, vacation information, and other paid time off information.
- **Performance and talent information:** qualifications, evaluations, developmental planning, and other talent management and team based assessments.
- **Background information:** educational, training, and employment background, and other background information commonly used for security screenings, subject to the requirements of applicable law.
- **Other information:** Employee Data specifying medical or health conditions, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, or Employee Data specifying the sex life of the individual.

The Employee Data will be provided to the Firm either by or on behalf of our clients.

IV. PURPOSE, USE AND DISCLOSURE OF EMPLOYEE DATA

The Firm uses and otherwise processes Employee Data to the extent necessary or appropriate for the performance of legal services for its clients. If an Employee does not agree to the uses and collection described herein, please immediately contact the Firm's Privacy Officer (described below).

With respect to Employee Data covered by the Privacy Shield (as defined below), discussed further below, the Firm certifies that it collects Employee Data solely to the extent such Employee Data is relevant to the purposes of performing legal services.

As part of normal business operations, the Firm may disclose Employee Data to service providers acting as data processors in connection with the Firm's performance of legal services for our clients (i.e., the Employee's employers. All such service providers are bound by contract to refrain from using the Employee Data for any purpose other than providing the service to the Firm. The Firm is liable under the Privacy Shield Principles (as defined below) for its third party providers to process transferred Employee Data in a manner consistent with the Privacy Shield Principles. The Firm may also share Employee Data with external advisors (e.g., experts, accountants, and auditors) of the Firm. The Firm seeks to (i) exercise appropriate due diligence in the selection of such service providers, and (ii) require via contract or otherwise that such service providers maintain adequate technical and organizational security measures to safeguard the Employee Data, and process the Employee Data only as instructed by the Firm.

The Firm may disclose or transfer Employee Data in connection with, or during negotiations of, any merger, acquisition, spin-off, sale of the Firm assets, product lines or divisions, any financing or any similar transaction. We may also disclose Employee Data to prevent damage or harm to us, our services, or any person or property, or if we believe that disclosure is required by law (including to meet national security or law enforcement requirements), or in response to a lawful request by public authorities. Except as described herein, we will not otherwise disclose Employee Data to third parties unless you have been provided with an opportunity to opt in to such disclosure.

V. OTHER PROCESSING REQUIRED BY LAW

In addition to the activities described above, the Firm may also process, disclose, and transfer Employee Data to governmental agencies and regulators (e.g., tax authorities), social organizations (e.g., a social benefits agency or social security organizations (e.g., pension funds)), courts and other tribunals, and government authorities to the extent permitted or required by applicable law.

VI. PRIVACY SHIELD

The Firm complies with the E.U.-U.S. Privacy Shield Principles and the Swiss-U.S. Privacy Shield Principles, including the Supplemental Principles (collectively, the "**Privacy Shield Principles**"), as set forth by the U.S. Department of Commerce regarding the collection, use and retention of personal information, including Employee Data, transferred from the E.U. to the U.S. and from Switzerland to the U.S., respectively, (the program being referred to as the "**Privacy Shield**"). The Firm has certified to the Department of Commerce that they adhere to the Privacy Shield Principles. If there is any conflict between the terms in this policy and the Privacy Shield Principles, the Privacy Shield Principles shall govern. To learn more about the Privacy Shield program, and to view our certification, please visit https://www.privacyshield.gov. A list of companies that are currently certified under the Privacy Shield is available at https://www.privacyshield.gov/list.

The Firm may, but shall not be required to, also process Employee Data relating to individuals in the E.U. and/or Switzerland via other compliance mechanisms, including data processing agreements based on the E.U. Standard Contractual Clauses. The Firm is responsible for the processing of personal data it receives, under the Privacy Shield, and subsequently transfers to a third party acting as an agent on its behalf. The Firm complies with the Privacy Shield Principles for all onward transfers of personal data from the EU and Switzerland, including the onward transfer liability provisions. The storage by the Firm of Personal Data on servers and/or on software made available or hosted by third party vendors shall not be considered disclosures of Employee Data to a third party so long as the third party vendor does not have direct access to the Personal Data stored or hosted.

The Firm is subject to the investigatory and enforcement powers of the U.S. Federal Trade Commission ("**FTC**"), and the Firm is committed to responding promptly to inquiries and requests by the United States Department of Commerce for information relating to the Privacy Shield Principles. The Firm adheres to the Privacy Shield Principles except, as required or allowed by law, to meet legal, governmental, law enforcement or national security obligations, or to protect the health or safety of an individual. The Firm maintains reasonable and appropriate administrative, physical and technical security measures designed to help protect against loss, misuse, and alteration of Employee Data. However, information transmitted on the Internet and/or stored on systems attached to the Internet is not 100% secure. As a result, we do not ensure, warrant or guarantee the security or integrity of such information.

In compliance with the Privacy Shield Principles, the Firm commits to resolve complaints about its collection or use of Employee Data. E.U. individuals with inquiries or complaints regarding our Privacy Shield policy should first contact the Firm's Data Protection and Privacy Officer at privacyofficer@lewisrice.com.

The Firm will comply with the Privacy Shield Principles, make reasonable efforts to accommodate employee privacy preferences, and will not use employees' exercise of their rights under the Privacy Shield to restrict employment opportunities or take punitive action against employees.

The Firm uses a self-assessment approach to assure compliance with this Policy and periodically verifies that the Policy is accurate, comprehensive for the information intended to be covered, is disseminated to the applicable employees, is completely implemented and accessible and is in conformity with the Privacy Shield Principles.

The Firm shall also, upon notice, take reasonable and appropriate steps to stop and remediate unauthorized processing by third party agents and agrees to provide a summary or representative copy of the relevant privacy provisions of its contracts to agents of the Department of Commerce upon request.

Where employees of our clients residing in the E.U. and/or Switzerland make complaints about violations of their Employee Data protection rights and are not satisfied with the results of our internal review, complaint, and appeal procedures, they will be directed to the state or national data protection or labor authority in the jurisdiction where the employees work. Under certain limited circumstances, E.U. and/or Swiss individuals may invoke binding Privacy Shield arbitration, as described here: https://www.privacyshield.gov/article?id=How-to-Submit-a-Complaint. The Firm commits to cooperate with applicable E.U. Data Protection Authorities and the Swiss Federal Data Protection and Information Commissioner (collectively the "***DPAs***") in the investigation and resolution of Privacy Shield complaints with regard to Employee Data transferred from a European country to the U.S. company and to comply with any advice given by the DPAs where such authorities take the view that we need to take specific action to comply with the Privacy Shield Principles.

VII. ACCESS TO EMPLOYEE DATA

Employees have the right to access, review, update, correct and request the deletion of their own Employee Data in accordance with applicable law, including the Privacy Shield Principles, and subject to certain limited exceptions. Employees also have the right to opt out of us using such employee's Employee Data for a purpose that is materially different from the purpose(s) for which it was originally collected or subsequently authorized by such employee. The Firm will respond to reasonable requests in an appropriate timeframe as determined by the applicable law governing the use of the applicable Employee Data. Employees should transmit any requests for access or updates to, or corrections or deletions of, their own Employee Data to Firm as specified below in Section IX.

The Firm will also contact users whose Employee Data is within the scope of the Privacy Shield Principles to obtain prior affirmative express consent if sensitive Employee Data (i.e., Employee Data specifying medical or health conditions, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, or Employee Data specifying the sex life of the individual) is to be disclosed to a third party, or if such sensitive Employee Data is to be used for a purpose other than those for which it was originally collected or subsequently authorized by such user. We will treat as sensitive any Employee Data received from a third party where the third party identifies and treats it as sensitive.

VIII. CHANGES

The Firm may amend this policy at any time. If the Firm makes any changes in the way it collects, uses, and/or shares Employee Data, we will notify affected employees by sending an email at the last email address that such employees provided to us.

IX. QUESTIONS

Employees who have any questions, comments or complaints about this Employee Data Privacy Policy or wish to (i) access, review, correct or request the deletion of their Employee Data or learn more about who has access to such information, (ii) make any other type of request, or (iii) report a concern or complaint related to Employee Data, should contact the Firm's Privacy Officer identified below.

Employees who reside in an European Union country or in Switzerland and who believe the Firm maintains their Employee Data within the scope of Privacy Shield certification may direct any questions or complaints to the Firm's Privacy Officer, whose contact information is below:

Data Protection and Privacy Officer

By email at privacyofficer@lewisrice.com

By mail at 600 Washington Avenue, Suite 2500, St. Louis, MO 63101 Attn: Data Protection and Privacy Officer.

The Firm is committed and required to respond to any inquiries on this issue within one (1) month of receiving the inquiry.

EFFECTIVE DATE: August 14, 2018