EU-U.S. Privacy Shield
Policy Statement
(Effective date: May 25, 2018)

Clinical Reference Laboratory, Inc. ("CRL") and its affiliates, adhere to the EU-U.S. Privacy Shield published by the U.S. Department of Commerce (the "Principles") concerning the transfer of Personal Data from the European Union ("EU") to the United States of America and is subject to the investigatory and enforcement powers of the Federal Trade Commission ("FTC"). If there is any conflict between the policies in this privacy policy and the Principles, the Principles shall govern.

To learn more about the EU-U.S. Privacy Shield program, and to view our certification, please visit www.privacyshield.gov/welcome.

This privacy policy outlines our general policy and practices for implementing the Principles, including the types of information we gather, use, and retain regarding your Personal Data and the Notice, Choice, Accountability for Onward Transfer, Security, Data Integrity and Purpose Limitation, Access, and Recourse, Enforcement and Liability pertaining to that Personal Data. This privacy policy applies to all Personal Data received by CRL whether in electronic, paper or verbal format.

This notice addresses Data Subjects whose Personal Data we may receive from one of our customers, suppliers or other business partners in the EU. When CRL receives Personal Data for processing pursuant to instructions of clients or their partners, we are acting as an agent for our client and do not provide notice to Data Subjects regarding the collection and use of their Personal Data. Our clients remain responsible for providing notice, if and to the extent they believe such notice is necessary under applicable EU law.

Definitions

"Data Subject" means the individual to whom any given Personal Data covered by this Privacy Shield Policy refers.

"Personal Data" - means any information relating to a Data Subject residing in the European Union that can be used to identify that individual either on its own or in combination with other readily available data.

"Sensitive Personal Data" means personal data regarding a Data Subject's race, ethnic origin, sexual orientation, political opinions, religious or philosophical beliefs, trade union membership or that concerns a Data Subject's health.

Principles

1. Notice

CRL notifies Data Subjects about its adherence to the EU-US Privacy Shield principles through its publicly posted website privacy policy, available at:

http://www.crlcorp.com/what-we-do/privacy-shield/

2. Collection & Use

CRL is a privately held clinical testing laboratory offering leading edge services in the areas of Pharmaceutical Trials, Employee Wellness, Molecular Diagnostics, Insurance Risk Assessment, and Drugs of Abuse Testing.

We will collect only as much Personal Data as we need for the specific purposes for which it was collected, we won't use it for other purposes without obtaining your consent, and keep your Personal Data only as long as we need it for the purposes for which we collected it, or as permitted by law.

- CRL may collect a person's name or initials, gender, race/creed/national origin, date of birth, email address, mailing address, telephone number, personal identification number, group/health insurance policy numbers and amounts, and medical information (including test results).
- CRL may share your Personal Data pursuant to a lawful request or for national security.
- CRL will use your Personal Data in support of the services we offer, communicating with corporate business partners about business matters, processing on behalf of our business customers, complying with contractual and legal obligations, and conducting related tasks for legitimate business purposes.

3. Accountability of Onward Transfer

CRL recognizes potential liability in cases of onward transfer to third parties.

CRL may provide Personal Data to third parties acting as agents, consultants, and contractors to perform tasks on behalf of and under our instructions. CRL will not transfer any Personal Data to a third-party without first ensuring that the third-party adheres to the Principles.

CRL does not transfer Client Personal Data to unrelated third parties, unless lawfully directed by a client, or in certain limited or exceptional circumstances in accordance with the EU-U.S. Privacy Shield Framework. For example, such circumstances would include disclosures of Personal Data required by law or legal process, or disclosures made in the vital interest of an identifiable person such as those involving life, health or safety.

In the event that CRL transfers Personal Data to an unrelated third party, CRL will ensure that such party is either subject to the EU-U.S. Privacy Shield Framework, subject to similar laws providing an adequate and equivalent level of privacy protection, or will enter into a written agreement with the third party requiring them to provide protections consistent with the EU-U.S. Privacy Shield Framework and CRL's EU-U.S. Privacy Shield policy.

Should CRL learn that an unrelated third party to which Personal Data has been transferred by CRL is using or disclosing Personal Data in a manner contrary to this Policy, CRL will take reasonable steps to prevent or stop the use or disclosure.

Personal Data is accessible only by those CRL employees and consultants who have a reasonable need to access such information in order for us to fulfill contractual, legal and professional obligations. All of our employees and consultants have entered into strict confidentiality agreements, and/or have been subjected to thorough criminal background checks.

4. Data Integrity & Security

CRL uses reasonable efforts to maintain the accuracy and integrity of Personal Data and to update it as appropriate. CRL has implemented physical and technical safeguards to protect Personal Data from loss, misuse, and unauthorized access, disclosure, alternation, or destruction.

5. Access

Upon reasonable request and as required by the Principles, CRL allows Data Subjects access to their Personal Data, in order to correct or amend such information where inaccurate.

To submit such requests or raise any other questions, please contact the business that provided your Personal Data. You may also contact our EU-U.S. Privacy Shield Contact listed below. We reserve the right to take appropriate steps to authenticate an applicant's identity, to charge an adequate fee before

providing access and to deny requests, except as required by the EU-U.S. Privacy Shield Framework.

To request erasure of Personal Data, Data Subject's should submit a written request to CRL's EU-U.S. Privacy Shield Contact.

6. **Annual Assessment**

CRL will renew its EU-U.S. Privacy Shield certifications annually, unless it subsequently determines that it no longer needs such certification or if it employs a different adequacy mechanism.

Prior to the re-certification, CRL will conduct an in-house verification to ensure that its attestations and assertions with regard to its treatment of Personal Data are accurate and that the company has appropriately implemented these practices.

7. Enforcement

Protecting Personal Data is of utmost importance to CRL. CRL commits to resolve complaints about your privacy and our collection or use of your Personal Data. Data Subjects with inquiries or complaints regarding this privacy policy should first contact CRL with questions, comments or complaints regarding CRL's EU-U.S. Privacy Shield or data collection and processing practices at:

CRL's EU-U.S. Privacy Shield Contact Information
Clinical Reference Laboratory, Inc.
Attn: Privacy Officer
8433 Quivira Road
Lenexa, KS 66215
privacy@crlcorp.com

If your inquiry is not satisfactorily addressed, you may contact the JAMS International Dispute Resolution Process. JAMS International will serve as a liaison with the CRL to resolve your concerns. http://www.jamsadr.com/eu-us-privacy-shield.

Data Subjects may complain to their home data protection authority and can invoke binding arbitration for some residual claims not resolved by other redress mechanisms.

If you have a comment or concern that cannot be resolved with us directly, you may contact the competent local data protection authority.