charles river

Policy Owner/Sponsor: IT and Legal
Review Date by Policy Review Committee: March 2016
Supersedes: January 15, 2013

Effective Date: March 2016

[To Be Completed by Policy Review Committee]

EU Data Privacy Policy

PURPOSE

It is our policy to respect the privacy of our employees, customers, business partners, and others.

POLICY

We collect, use, retain and otherwise process Personal Data in a manner consistent with the laws of the countries in which we do business.

In furtherance of this commitment, while it was in effect, CRL US complied with the US-EU Safe Harbor Framework as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of personal data from European Union countries ("EU"). The Safe Harbor Framework was invalidated on October 6, 2015 by a ruling of the Court of Justice of the European Union.

Although we can no longer rely on the Safe Harbor Framework to legitimize our transfers of personal data, we continue to adhere to fundamental EU data protection principles of notice, choice, onward transfer, security, data integrity, access and enforcement (summarized below under the heading "EU Data Protection Principles"). We will evaluate the new US-EU Privacy Shield framework if and when it is adopted by the EU.

In the meantime, and until further notice, the CRL Group will rely on other legal bases for the transfer of personal data from the EU to the US, including the EU Commission's Standard Clauses. CRL US may act as a controller or as a processor, depending on the circumstances.

If we have entered into Standard Clauses with regard to particular personal data, we will comply with our obligations under the Standard Clauses. Those obligations may be more specific than the EU Data Protection Principles summarized below, or cover additional topics.

OUR PERSONNEL

THE KINDS OF PERSONAL DATA WE COLLECT AND WHAT WE DO WITH IT

We collect, process, and retain Personal Data concerning our employees and their family members (including retirees and past employees and their family members to whom we have ongoing obligations such as paying benefits), and in some cases our non-employee agents (such as freelance contractors). The types of Personal Data that we may collect include:

- name
- gender
- date of birth
- home address
- business phone number (private phone number is optional)
- business email-address (private email-address is optional)
- social security/national insurance or similar government-issued ID number
- marital status
- language preference
- emergency contact
- dependents
- employee movement (hire, transfer, promotion, salary changes, demotions, terminations, etc.)
- positions held
- salary information
- location
- job codes
- reports / reporting relationship (if any)
- salary grade
- pay groups
- incentive plan
- stock eligibility

We process personnel Personal Data for the following purposes:

- determining, evaluating and implementing employment-related actions and obligations;
- designing, evaluating and administering compensation, benefits and other human resources programs;
- designing, evaluating and implementing employment-related education and training programs;
- monitoring and evaluating employee conduct and performance; and

- maintaining plant and employee security, health and safety.

Most decisions about the use of Personal Data from the EU (as described above) will be made by the CRL Group members located in the EU. Personal Data may be transferred to CRL US to facilitate and support human resources functions that are performed by our EU entities, and to provide network, application, and email access to employees of our EU entities. (and in this case, CRL US would be acting as a data processor for its EU entities).

However, CRL US may sometimes consult with our EU entities and review Personal Data together, in which case CRL US may act as a joint data controller. Such less-common situations could include consultations for the following purposes:

- discussing actual or potential litigation, legal compliance risks and other legal matters;
- discussing internal disciplinary proceedings, outcomes and policies;
- ensuring compliance with corporate policies and considering changes to corporate policies;
- monitoring global headcount and making decisions concerning roles, staffing, redundancies and recruitment;
- establishing and monitoring progress towards human resources diversity objectives;
- interactions with trade unions or work councils; and
- CRL Group company, business division, team and/or employee performance metrics.

CUSTOMERS AND OTHER BUSINESS CONTACTS

THE KINDS OF PERSONAL DATA WE COLLECT AND WHAT WE DO WITH IT

The kinds of Personal Data that we may collect about our past, present and potential customers, suppliers, contractors, joint venture partners and other business associates ("Business Contacts") are limited to name, position/responsibilities (e.g., Head of Procurement) and contact details (such as a business e-mail address and telephone number).

We collect, process, and retain Personal Data concerning our Business Contacts for the following purposes:

- collecting and storing customer information;
- maintaining business records relating to past, present and potential customers, suppliers, contractors, joint venture partners and other business associates;
- conducting auditing, accounting, financial and economic analyses;
- facilitating business communications, negotiations, transactions, conferences and compliance with contractual and legal obligations;
- providing goods and services to our customers; and

- monitoring our website, which includes processing orders and engaging in transactions and communications.

EU DATA PROTECTION PRINCIPLES

The following summary of EU Data Protection Principles is provided to help EU individuals understand their rights and our obligations with respect to their Personal Data. As we mentioned above, if the standard clauses that we have entered into, or applicable law, require more specific or additional obligations, then we will comply with those obligations.

Notice

Where we collect Personal Data directly from individuals in the EU, we will inform them about the purposes for which we collect and use such Personal Data, the types of non–agent third parties to which we disclose that information, the choices and means, if any, we offer individuals for limiting the use and disclosure of their Personal Data, and how to contact us. Notice will be provided in clear and conspicuous language when individuals are first asked to provide Personal Data to us, or as soon as practicable thereafter, and in any event before we use or disclose the information for a purpose other than that for which it was originally collected.

Where we receive Personal Data from our subsidiaries, affiliates or other entities in the EU, we will use and disclose such information in accordance with the notices provided by such entities and the choices made by the individuals to whom such Personal Data relates.

Choice

We offer individuals the opportunity to choose whether their Personal Data is (1) to be disclosed to a non-agent third party, or (2) to be used for a purpose that is incompatible with the purpose for which it was originally collected or subsequently authorized.

For Sensitive Data, individuals must affirmatively and explicitly consent to the disclosure of the information to a non-agent third party or the use of the information for a purpose other than the purpose for which it was originally collected or subsequently authorized, unless such new use or transfer is (1) in the vital interests of the individual or another person where the data subject is physically or legally incapable of giving his consent; (2) necessary for the establishment of our legal claims or defenses; (3) required to provide medical care or diagnosis where the data is processed by a health professional subject under national law or rules established by national competent bodies to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy; (4) necessary to carry out our obligations in the field of employment law in so far as it is authorized by applicable national legislation providing for adequate safeguards; or (5) related to data that is manifestly made public by the individual.

We provide individuals with reasonable mechanisms to exercise their choice. For example, if we send an individual a direct marketing e-mail, that e-mail will contain a link so the individual can easily opt-out of future direct marketing e-mails.

Transfers to Agents

If we transfer Personal Data to our Agents, we first ascertain whether the Agent is subject to the EU 95/46/EC Directive or another adequacy finding or we will enter into a contract obligating the Agent to provide at least the same level of protection as is required by the relevant EU Data Protection Principles

as described above. We also follow any additional requirements of the Standard Clauses with respect to agents. Where we have knowledge that an Agent is using or disclosing Personal Data in a manner contrary to this policy, we take reasonable steps to prevent or stop the use or disclosure.

Security

We take reasonable and appropriate precautions to protect Personal Data in our possession from loss, misuse, alteration, destruction, or unauthorized access or disclosure. We take special care to protect Sensitive Data.

Data Integrity

We use Personal Data only in ways that are compatible with the purposes for which it was collected or subsequently authorized by the individual. We take reasonable steps to ensure that Personal Data is relevant to and reliable for its intended use, accurate, complete, and current.

Access

Upon request, we provide individuals with access to their Personal Data. Individuals may request corrections, deletions, or additions, as appropriate, except where the burden or expense of providing such access would be disproportionate to the risks to the individual's privacy or would violate another individual's rights.

Automated Decision-making

An "automated decision" means a decision by us that produces legal effects concerning a person or significantly affects a person and which is based solely on automated processing of personal data intended to evaluate certain personal aspects relating to that person, such as his or her performance at work, creditworthiness, reliability, conduct, etc. We will not make any automated decisions concerning any individual, except when one of the following apply: (1) We make the decision in order to enter into or perform a contract with the individual, and the individual is given an opportunity to discuss the results of a relevant automated decision with our representative, or (2) the decision is permitted or required by the laws of the EU country from which the personal data was received.

Enforcement

We conduct a self-assessment of relevant privacy practices to verify adherence to this policy at least once per year. Any employee we determine is in violation of this policy will be subject to disciplinary actions.

We investigate and attempt to resolve complaints regarding use and disclosure of Personal Data in accordance with this Policy. For complaints that cannot be resolved between us, we will comply with the requirements in the applicable Standard Clauses.

LIMITATION ON APPLICATION OF PRINCIPLES

Adherence by us to the EU Data Protection Principles may be limited (1) to the extent required to respond to a legal obligation or to enforce our legal rights; (2) to the extent necessary to meet lawful requests for information under national security laws or for purposes of law enforcement; and (3) to the extent expressly permitted by an applicable law, rule, or regulation of the country from which the personal data originated.

WEBSITE PRIVACY

We see the Internet and the use of other technology as valuable tools to communicate and interact with customers, employees, healthcare professionals, business partners, and others. We recognize the importance of maintaining the privacy of information collected online and have created a specific Website Privacy Policy (WPP) governing the treatment of Personal Data collected through websites that we operate. With respect to Personal Data that is transferred from the EU, the WPP is subordinate to this policy. However, the WPP also reflects additional legal requirements and evolving standards with respect to privacy.

GENERAL

The Company reserves the right to amend or terminate this Policy as the Company deems necessary or warranted in accordance with applicable laws.

SCOPE

This policy applies to all subsidiaries and affiliates of Charles River Laboratories, Inc. located at 251 Ballardvale Street, Wilmington, Massachusetts, 01887, United States of America ("CRL US"), our corporate affiliates located in the European Economic Area, and all other affiliates globally (collectively, including CRL US, the "CRL Group"). It sets forth the principles under which we manage the processing of Personal Data collected in the EU and subsequently transferred to the United States in any format, including electronic, paper, or verbal.

DEFINITIONS

For the purposes of this policy, the following definitions apply:

- "**Agent**" means any third party that collects or uses Personal Data under the instructions of, and solely for, us or to which we disclose Personal Data for use on our behalf.
- "**Personal Data**" means information that identifies or describes an identified or identifiable living natural person including, but not limited to, address, credit card information or bank statement.
- "**Sensitive Data**" is a subset of Personal Data and means information pertaining to an individual's racial or ethnic origin, political opinions or religious or philosophical beliefs, medical or health conditions, trade memberships or sex life.
- **"Standard Contractual Clauses"** are contracts that have been approved by the EU Commission to govern the transfer of personal data from the EU to the US. There are two main sets of the Standard Clauses. One deals with "controller" to "processor" transfers and the other set deals with "controller" to "controller" transfers.
- **"Controller"** is someone who makes decisions about what personal data is collected, the purposes for which it is processed, and so on

- **"Processor"** is someone who implements a controller's instructions about processing personal data (for example, an IT service provider)

RESPONSIBILITIES

Any questions related to the interpretation of this Policy and/or a subject matter included in this Policy shall be directed to the Chief of Information Security and Compliance and the Corporate Legal Department.

Any questions or concerns regarding the use or disclosure of Personal Data should be directed to our Chief of Information Security and Compliance, Charles River Laboratories International, Inc., 251 Ballardvale Street, Wilmington, Massachusetts 01887 or 781-222-6000 or via dataprivacy@crl.com.

RELATED DOCUMENTS

Standard Contractual Clauses

Website Privacy Policy (WPP)