



PRGX Global, Inc.

***Global Employee Privacy Statement***

*April 26, 2023*

PRGX Global, Inc. and its affiliates and subsidiaries (collectively referred to in this Statement as “PRGX,” “we”, “our”, or “us”) is committed to protecting the privacy of our employees and job applicants and we are equally committed to the proper handling of the Personal Data collected or generated in connection with your employment or application for employment as well as respecting your individual rights with respect to your information.

**The PRGX entity (PRGX affiliate) that employs you or engages your services, or with which you interacted, shall act as data controller for any Personal Data (defined below) collected or generated in connection with your employment or application for employment.**

This Employee Privacy Statement (“Statement”) explains our practices with regard to Personal Data of current, former and potential employees, including job applicants, interns, temporary workers (“you”, “your”, or “employee”). This Statement may be updated from time to time to reflect changes in our Personal Data practices, and we will post a prominent statement on the Employee Intranet Site or PRGX career sites that collect applicant information to notify you of any significant changes.

**1. DEFINITIONS**

***Personal Data*** (“Personal Data”) is any information relating to an identified or identifiable natural person (“data subject”); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

***Sensitive Personal Data*** (“Sensitive Personal Data”) means Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

**2. INFORMATION WE COLLECT**

We may collect Personal Data, either directly from you or from third parties including public databases, social media platforms, recruitment companies or companies performing background checks or other screening. We collect, process, and transfer employee Personal Data through electronic and paper-based data processes. We have established routine processing for certain functions relating to your employment (such as processing for regular payroll and benefits administration). We also process employee Personal Data on an occasional or ad hoc basis (such as when an employee is being considered for a new position).

In the normal course of activities, we collect the following types of Personal Data:

- Personal identification information, such as your name, home address, date of birth, gender, work-related photographs, and home phone number;
- Government-issued identification numbers, such as SSN or national insurance number for payroll and benefits purposes;
- Sickness absence and health information, fit notes, medical certificates including COVID-19 vaccination records and testing results to the extent allowed by employment law and laws and rules related to the prevention of COVID 19 infection, as applicable from time to time;
- Immigration, right-to-work and residence status, to the extent allowed by employment law;
- Family and emergency contact details;
- Job-related information, such as years of service, work location, employment ID, work record, vacation absences, and contract data;
- Educational and training information, such as your educational awards, certificates and licenses, vocational records and in-house training attendance;
- Recruitment and performance-related data, such as objectives, ratings, comments, feedback results, career history, work equipment, career and succession planning, skills and competencies and other work-related qualifications;
- Information related to your usage of our assets;
- Information needed for compliance and risk management, such as disciplinary records, background check reports and security data; and
- Payroll- and payment- or benefits-related information, such as salary and insurance information, dependents, government identifier or tax numbers, bank account details, and employment related benefits information.

***Additional information for California employees.*** The California Consumer Privacy Act (CCPA) requires us to identify the specific CCPA categories of Personal Information that we collect. The information we collect, as described above, falls into the following CCPA categories:

- Identifiers
- Protected classifications
- Internet activity information
- Professional and employment-related information
- Education information
- Audio or visual Information
- Inferences drawn from any of the above information categories

### **3. HOW WE USE YOUR INFORMATION**

We take reasonable steps to ensure that the Personal Data we process is reliable for its intended use, is accurate, up-to-date and complete, and is limited to the Personal Data required to carry out the purposes of the processing, as described in this Statement. Where appropriate, we may ask you to ensure that your Personal Data that we hold is accurate and up to date.

We process employee Personal Data for the following legal bases and purposes:

- (1) **To Perform the Employment Contract We Have with You or to Take Steps to Enter into a Contract with You:** recruitment and staffing, administration of compensation and benefits programs, to assess your suitability for a particular position, advancement and succession planning, performance management and training;
- (2) **To Comply with Our Legal Obligation as Your (Potential) Employer:** legal and regulatory compliance (including compliance with government authority requests for information, liens, garnishments and tax compliance) and risk management, workplace and workforce management and administration (such as travel and expense programs, internal health and safety programs, including federal and state COVID-19 safety protocols) and internal reporting and audit, and to conduct ongoing compliance screenings against publicly available watch and sanction lists (including the performance of background checks);
- (3) **To Facilitate our Employment Relationship, Secure, our Network and Other Legitimate Business Interests:** protection of our company, our workforce, and the public against injury, theft, legal liability, fraud or abuse, or threat to the security of our networks, communications, systems, facilities and infrastructure and other customary and legal business-related purposes (see PRGX Acceptable Use Policy for further details); and
- (4) **Based on Your Consent:** In some specific and limited circumstances, we process your Personal Data based on your consent.

We process employee Sensitive Personal Data if it is needed for legitimate business objectives and to the extent permitted or required to comply with applicable law. Sensitive Personal Data will not be collected, processed or transferred, except where adequate privacy protection mechanisms are in place and after having first obtained your informed consent, if required by law.

#### **4. YOUR PERSONAL DATA RIGHTS**

You may have certain rights with respect to our processing of your Personal Data, which include:

- (1) **Access, Correction and Transmission:** You may reasonably access the Personal Data pertaining to you that is on file with us. You also have the right to request that we correct incomplete, inaccurate or outdated Personal Data. To the extent required by applicable law, you may also request that we transmit Personal Data you have provided to us to you or to another company.
- (2) **Objection:** We respect your right to object to any uses or disclosures of your Personal Data that are not (i) required by law, (ii) necessary for the fulfillment of a contractual obligation (your employment contract), or (iii) required to meet legitimate interests of PRGX as an employer (such as general human resource administration disclosures for auditing and reporting purposes, internal investigations, management of network and information systems security, or protection of our assets). If you do object, we will work with you to find a reasonable accommodation. You may also withdraw your consent at any time in relation to our processing of Personal Data based on your consent.
- (3) **Deletion:** You may request the deletion of your Personal Data as provided by applicable law. This applies, for instance, where your information is outdated; where the processing is not necessary or is unlawful; where you withdraw your consent to our processing

based on such consent; or where we determine we should accommodate an objection you have raised to our processing. In some situations, we may need to retain your Personal Data pursuant to our legal obligations or for the establishment, exercise or defense of legal claims.

- (4) **Restriction of Processing:** Similarly, and where provided by applicable law, you may request that we restrict processing of your Personal Data while we are answering your request or complaint pertaining to (i) the accuracy of your Personal Data, (ii) our legitimate interests to process such information, or (iii) the lawfulness of our processing activities. You may also request that we restrict processing of your Personal Data if you wish to use the Personal Data for litigation purposes.

If you wish to exercise these rights, you may contact your local Human Resources manager or the PRGX Privacy Office as described below in the “How to Contact Us” section. To access **PRGX’s Personal Data Rights Request Forms** click here.

Where reasonable, we will accommodate your request. However, PRGX may charge a reasonable fee or refuse to act on a request if it is manifestly unfounded or excessive in particular because of its repetitive character. In some situations, PRGX may refuse to act or may impose limitations on your rights if, for instance, your request is likely to adversely affect the rights and freedoms of PRGX or others, prejudice the execution or enforcement of the law, interfere with pending or future litigation, or infringe applicable law. In all cases, you have a right to file a complaint with the applicable Data Protection Authority.

## **5. DISCLOSURES OF PERSONAL DATA**

We may disclose your Personal Data for legitimate purposes to the following recipients:

- (1) among our affiliated companies (including our subsidiaries and branches) for purposes stated in this Statement;
- (2) to third party vendors, whom we contract with for specific purposes;
- (3) to companies who provide benefits and services to you (such as retirement plans);
- (4) to a newly formed or acquiring organization if PRGX is involved in a merger, sale or a transfer of some or all of its business;
- (5) to public authorities in response to lawful requests to meet national security or law enforcement requirements;
- (6) where otherwise required by law; or
- (7) where permitted by law, such as with your consent or in the event of an emergency.

## **6. INTERNATIONAL DATA TRANSFERS**

Personal Data may be transferred outside of the country of origin for purposes described in this Statement. For Personal Data that originates from the European Economic Area (“EEA”) or the UK, this may include transferring Personal Data outside the EEA or the UK to locations in the United States (“U.S.”) and other countries that have different data protection laws than those in the country of origin and that may not have been granted an adequacy decision by the European

Commission or the Information Commissioner's Office in the UK.

In this regard, for any such Personal Data subject to EU or UK data protection laws, PRGX takes measures designed to provide the level of data protection required in the EU and UK, including ensuring transfers are governed by the requirements of the Standard Contractual Clauses adopted by the European Commission or another adequate transfer mechanism. PRGX entities have also entered into intragroup transfer agreements based on the Standard Contractual Clauses which allows for the processing and transfer of Personal Data. In addition, PRGX USA, Inc. is subject to the investigatory and enforcement powers of the Federal Trade Commission, or any other U.S. authorized statutory body.

For further information, and to obtain a copy of the relevant data transfer mechanism, please contact us through the "How to Contact Us" section below.

## **7. YOUR OBLIGATIONS**

Bear in mind that you have responsibility for the accuracy of your Personal Data. Please let us know when changes to your Personal Data are needed by contacting your local Human Resources manager. We will use reasonable efforts to respond to all such requests in a timely manner.

## **8. SECURITY AND DATA INTEGRITY**

PRGX is committed to protecting the privacy, confidentiality and security of the data that is provided to us, including Personal Data, through a combination of technical, physical and administrative measures, controls, policies, practices and procedures.

PRGX's privacy and security framework is based on ISO 27001 standards and, as such, we have a strong focus on establishing, maintaining, and continuously improving information security management systems and identifying, analyzing, and addressing information security risks. The ISO 27001 standards cover all aspects of security including physical protection of equipment and people, hiring practices, employee training, network security, and access controls. This framework combined with regular monitoring and testing of controls, allows us to ensure that appropriate levels of data confidentiality, integrity, and availability are maintained.

Not only are we committed to protecting your Personal Data, we are also committed to protecting and respecting the privacy of our clients, our suppliers and vendors, our investors and those individuals who browse and use our websites. Employees are expected to follow the company's privacy and security policies and procedures, as well as applicable laws, when accessing and handling all Personal Data as well as confidential information provided to us by our clients, suppliers, investors, and visitors of our websites. When we retain a third-party service provider, that provider will be required to (i) use measures to protect the confidentiality and security of the Personal Data and (ii) process the Personal Data only as directed by PRGX.

## **9. DATA RETENTION**

We will retain your Personal Data only for as long as necessary to achieve the purposes outlined in this Statement, usually for the duration of any contractual relationship and for any period thereafter as legally required or permitted by applicable law. This means that, in some cases, we

may be required to retain your Personal Data for a period of time following termination of your relationship with us. Our retention policies reflect all applicable domestic and international law, including relevant statute of limitation periods and other legal requirements

## **10. HOW TO CONTACT US**

Questions about how PRGX is using Personal Data or if you would like to invoke your Personal Data rights as set forth in this Statement, may be sent by email to [privacyoffice@prgx.com](mailto:privacyoffice@prgx.com) or by contacting:

### **Alicia Jackson**

Chief Compliance Officer  
200 Galleria Parkway, Suite 450  
Atlanta, GA 30339  
USA  
770-779-3042  
[alicia.jackson@prgx.com](mailto:alicia.jackson@prgx.com)

For unresolved privacy complaints relating to such Personal Data, PRGX has further committed to cooperate with any applicable dispute mechanisms established by EU and UK regulatory authorities, including local data protection authorities, and to provide this recourse free of charge. If you do not receive timely acknowledgement of your complaint, or if your complaint is not satisfactorily addressed, please contact such applicable regulatory authority directly for further information.

## **11. CHANGES TO THIS STATEMENT**

**September 24, 2019:** Updated to ensure Statement remains compliant with the Privacy Shield Principles after the UK's withdrawal from the EU.

**November 11, 2021:** Updated to reflect the European Court of Justice's invalidation of EU-US Privacy Shield Framework and to add CCPA compliance requirements.

**September 20, 2022:** Updated to provide additional clarity around the definition of Personal Data and to ensure compliance with Italian privacy laws.

©2023 PRGX Global, Inc. All rights reserved. Many of the trademarks and service marks appearing on this website are registered trademarks. Use of this site is subject to certain Terms of Use which constitute a legal agreement between you and the Company. By using this site, you acknowledge that you have read, understood, and agree to be bound by the Terms of Use. Please review the Terms of Use; and if you do not agree to the terms, please do not use this site.