ADP Global Privacy Policy

Automatic Data Processing, Inc. and its Group Companies ("ADP", "us", "we") is committed to being transparent about its data processing activities and to protecting all Personal Data that is entrusted to us by ADP Associates, Contingent Workers and job applicants, client employees and workers, and business contacts such as Clients, prospects, consumers, website users or vendors ("Individuals").

ADP has adopted Binding Corporate Rules (BCR) Codes which establish the rules for Processing Personal Data at ADP either as a Data Processor or as a Data Controller.

When serving as a Data Processor, ADP shall only process Personal Data of Individuals in accordance with its Client Service Agreement and other instructions that it receives from its Clients. Where applicable, ADP shall also comply with its Binding Corporate Rules Code for Client Data Processing Services (the Processor Code) which provides the primary legal basis for transfers of Personal Data of Individuals from European locations to ADP Group Companies located outside of the European Economic Area (EEA).

Capitalized words in this document are defined in the Glossary provided under section IV below.

I. ADP's Privacy Principles

A. Providing Notice and Transparency

ADP publishes Privacy Statements to explain its Data handling practices to those Individuals for whom Personal Data is Processed by ADP. A Privacy Statement will be available when ADP collects Personal Data from the Individual as a Data Controller, and will also be provided upon request, in accordance with the applicable BCR Code.

B. Providing Choice and Obtaining Consent

ADP is committed to respecting the choices of Individuals regarding the Processing of their Personal Data. ADP provides Individuals with opportunities to choose how their Personal Data is Processed, as outlined in the respective BCR Codes. ADP will Process Personal Data in accordance with the approved Business Purposes outlined in the respective BCR Codes, and the scope of the Processing is limited to the applicable Business Purpose.

When a new or different Business Purpose is identified for Processing Personal Data, an evaluation of the Processing is required to determine if it is permissible. In some cases, consent from the Individual may be required.

C. Collecting and Using Personal Data

The collection and use of Personal Data is limited to those elements that are reasonably needed to achieve the specific Business Purpose and ADP strives to use Personal Data that are accurate, current and complete, consistent with the Business Purpose.

Additionally, Sensitive Personal Data may include Special Categories of Data which may only be Processed under certain circumstances as described in the BCR Codes.

D. Accessing and Correcting Personal Data
ADP is committed to providing Individuals with a reasonable opportunity to examine their own Personal Data and to update it if it is incorrect. Subject to any limitations provided by Applicable Law, ADP will provide Individuals with a copy of their Personal Data that is maintained by ADP under our Workplace Code or our Business Data Code.

When Processing Personal Data on behalf of its Client, ADP will support and assist the Client in addressing Individuals' requests, in accordance with the terms of the Service Agreement between ADP and the Client.

ADP also complies with other Individual rights as required by Applicable Law. Where reasonable, ADP will also provide other information that may be requested by an Individual, such as the source of the Personal Data or the Business Purposes for which ADP Processes Personal Data and other information that may be required by Applicable Law.

E. Accuracy and Retention of Personal Data
ADP is committed to setting appropriate standards for both the quantity and quality of the Personal Data that it processes. Reasonable measures are used to keep Personal Data appropriately accurate, complete and up-to-date, as needed for the Processing being performed. In many cases, ADP will rely on Individuals to use their own ability to access and correct Personal Data to ensure the accuracy of the Data.

ADP has implemented a Global Records Information Management (RIM) Policy and has established records retention schedules for Personal Data that ADP processes. Personal Data is retained in accordance with the records retention schedules to ensure that records containing Personal Data are retained as needed to fulfill the applicable Business Purposes, or to comply with applicable laws.

F. Protecting Personal Data while it is transferred to Third Parties
Personal Data may be transferred across national borders in compliance with laws that regulate cross-border data transfers and with adequate protection for the information. The BCR Codes and, if applicable, any Services Agreements, specify when and how Personal Data may be transferred to Third Parties. Where applicable, ADP will transfer Personal Data to Third Parties on behalf of our Clients as permitted by our Processor Code. As a Data Controller, ADP will transfer Personal Data as permitted by the approved Business Purposes defined in our Workplace Code and Business Data Code. When ADP, as a Data Processor, transfers Personal Data, the Processor Code ensures adequate levels of protection for the transfer of Personal Data from the EEA to outside jurisdictions.

ADP may disclose Personal Data to Third Party Processors that have been reviewed by ADP's Global Security Organization for privacy and security compliance and that are bound by a written service agreement with ADP containing appropriate privacy and security terms.

II. Compliance

A. Privacy by Design

Privacy by Design requires that privacy and data protection controls be built into new products and services that ADP offers. ADP has implemented the standards and procedures for ADP Associates and Contingent Workers who develop products or services for ADP.

B. Security Incidents

Within ADP's Global Security Organization, comprehensive enterprise-wide policies and procedures are in place for managing, tracking and reporting security incidents. ADP's security policies require logging of all actual security incidents reported to ADP by Associates, Clients or other third parties. Once a security incident is reported, ADP's incident response process is designed to ensure that all incidents are addressed in a timely and effective manner and in accordance with ADP security policies, procedures, and legal requirements. When necessary, procedures for the notification of Clients, Individuals and all other parties who may be impacted by the incident are initiated, and appropriate remedial actions are taken.

III. Governance

ADP's privacy program is managed by ADP's Global Chief Privacy Officer and the members of the Global Data Privacy and Governance Team in cooperation with the Privacy Stewards of all ADP's business units and functional areas. In addition, ADP has implemented a Privacy Network comprised of the members of the Global Data Privacy and Governance Team and other members of the Legal department, including compliance professionals and Data Protection Officers, who are in charge of privacy within their respective regions, countries, business units or functional areas.

IV. Glossary

ADP (ADP Group)	ADP (the ADP GROUP) means, collectively, Automatic Data Processing, Inc. (the Parent Company) and the Group Companies, including ADP, LLC.
Applicable Law	APPLICABLE LAW means any privacy or data protection laws that are applicable to any particular Processing activities.
Associate	ASSOCIATE means an Applicant, a current ADP employee, or a former ADP employee.
Binding Corporate Rules	BINDING CORPORATE RULES means a privacy policy of a group of related companies considered to provide an adequate level of protection for the transfer of Personal Data within that group of companies under Applicable Law.
Business Purpose	BUSINESS PURPOSE means a legitimate purpose for Processing Personal Data as specified in Article 2, 3 or 4 of any ADP Code, or for Processing Special Categories of Data as specified in Article 4 of any ADP Code.
Client	CLIENT means any company that utilizes one or more ADP products or services in the course of its own business.
Code	CODE means (as applicable) the ADP Privacy Code for Business Data, the ADP Workplace Privacy Code (internal to ADP), and the ADP Privacy Code for Client Data Processing Services; collectively referred to as the Codes.
Contingent Worker	CONTINGENT WORKER means an Individual who provides services to ADP (and who are subject to ADP's direct supervision) on a provisional or non-permanent basis, such as temporary workers, contract workers, independent contractors, or consultants.
Data Controller	DATA CONTROLLER means the entity or natural person which alone, or jointly with others, determines the purposes and means of the Processing of Personal Data.
Data Processor	DATA PROCESSOR means the entity or natural person which Processes Personal Data on behalf of a Data Controller.
Individual	INDIVIDUAL means any identified or identifiable natural person whose Personal Data are Processed by ADP either as a Data Processor or a Data Controller.

Personal Data or Data	PERSONAL DATA or DATA means any information relating to an identified or identifiable Individual. Personal Data may also be referred to as personal information in policies and standards that implement the Codes.
Privacy Network	PRIVACY NETWORK means the members of the Global Data Privacy and Governance team and other members of the Legal department, including compliance professionals, and Data Protection Officers who are in charge of privacy compliance within their respective regions, countries, Business Units or Functional areas.
Privacy Steward	PRIVACY STEWARD means an ADP executive who has been appointed by a Responsible Executive and/or ADP's Executive Leadership to implement and enforce the Privacy Codes within an ADP Business Unit.
Processing	PROCESSING means any operation that is performed on Personal Data, whether or not by automatic means, such as collection, recording, storage, organization, alteration, use, disclosure (including the granting of remote access), transmission, or deletion of Personal Data.
Services Agreement	SERVICES AGREEMENT means any contract, agreement, or terms pursuant to which ADP provides Client Services to a Client.
Sensitive Personal Data	SENSITIVE PERSONAL DATA is a subset of personal data that has been classified by law or by ADP policy as deserving additional privacy and security protections. Sensitive personal data includes things such as government-issued identification numbers, individual financial account numbers, individual medical records, genetic information and biometric information, and consumer reporting data, including employment background screening reports.
Special Categories of Data	SPECIAL CATEGORIES OF DATA means Personal Data that reveal an Individual's racial or ethnic origin, political opinions or membership in political parties or similar organizations, religious or philosophical beliefs, membership in a professional or trade organization or union, physical or mental health including any opinion thereof, disabilities, genetic code, addictions, sex life, criminal offenses, criminal records, or proceedings with regard to criminal or unlawful behavior.
Third Party	THIRD PARTY means any person, private organization, or government body that is not an ADP Company.
Third Party Processor	THIRD PARTY PROCESSOR means a Third Party that Processes Personal Data on behalf of ADP that is not under the direct authority of ADP.