ADP BIOMETRIC INFORMATION PRIVACY POLICY

ADP is committed to ensuring that security safeguards are in place to ensure that any biometric data that ADP possesses as a result of ADP's operations or of ADP clients' and client employees' use of ADP products and services is protected as required under applicable federal, provincial, state and/or territorial laws.

ADP's clients are responsible for developing and complying with their own biometric data handling practices and policies as may be required under applicable law.

Biometric Data Defined

Biometric Data means any biological characteristics of an individual, or information based on or derived from such a characteristic or measurements, that can be used to identify or authenticate that individual and as may be defined in other applicable local laws that govern the collection, use, storage or disclosure of biometric data. Biometric Data includes a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry regardless of how it is captured, converted, stored, or shared when such information is used to identify or authenticate the individual.

Collection, Storage, Use, Access, and Transmission of Biometric Data

ADP and/or its vendors will collect, store, use and/or transmit any Biometric Data solely for identity verification, workplace security, and fraud prevention. Neither ADP nor its vendors will sell, lease or trade any Biometric Data that it receives from clients or client employees as a result of their use of ADP products and services.

ADP Timekeeping Uses

ADP clients are responsible for compliance with applicable law governing any collection, storage, use, and/or transmission of Biometric Data they conduct or facilitate for their own business purposes, including regulatory reporting requirements, conducting privacy impact assessments and complying with other relevant legal obligations. To the extent required by law, ADP clients will obtain express required consents (including any written consents where required) from each employee for the client and will ensure that such consent is valid, complies with applicable law and authorizes the client, ADP and/or ADP's authorized licensors or vendors to collect, store, use, and/or transmit Biometric Data for the purposes specified in this policy.

Non-Timekeeping Uses

ADP and/or its vendors also may collect, store, use and/or transmit Biometric Data during the course of conducting ADP's operations or providing products or services to ADP's clients, client employees, consumers or ADP associates or contractors (collectively referred to as the user). With respect to Biometric Data collected, stored, used and/or transmitted by ADP and/or its vendors, to the extent required by law, ADP and/or its vendors will obtain all required consents (including any written consents where required) from each individual prior to the collection of such data.

Disclosure

ADP will not disclose, disseminate and/or transmit any Biometric Data to any person or entity other than the client and ADP's vendors without/unless:

a) First having the user's express consent;
b) The disclosed information completes a financial transaction authorized by the user;
c) Disclosure is required by state, provincial/territorial or federal law; or
d) Disclosure is required pursuant to law, a valid regulatory or governmental request, court order, warrant or subpoena.

Retention Schedule

ADP Timekeeping Uses

ADP will retain Biometric Data in ADP's and/or its vendor's possession or control until the client notifies ADP that it is terminating its services with ADP, the client or a client employee directly requests ADP to delete the individual's Biometric Data, or the client requests to discontinue use of the biometric technology for a specific employee. If ADP does not receive a deletion request, the Biometric Data will be destroyed in accordance with ADP's client services agreement or ADP's applicable record retention schedules, whichever is shorter. Client employees will not have direct access to rectify or delete their Biometric Data. Biometric Data can be deleted upon request by the client employee to their employer.

Non-Timekeeping Uses

Where Biometric Data is collected from client employees and consumers for ADP system authentication purposes (e.g. account set up, ID verification) data will be retained in accordance with applicable law for no longer than 3 years.

ADP Associates or Contractors

ADP and/or its vendors will retain any ADP associate's or contractor's Biometric Data in ADP's and/or its vendor's possession generated in the course of conducting ADP operations, including use of company-owned devices, until the ADP associate's employment terminates, or in the case of a contractor, until the vendor notifies ADP that it has terminated the contractor's assignment with ADP, the vendor asks ADP to delete contractor's Biometric Data, or the individual requests that such Biometric Data be destroyed without delay. Where Biometric Data is used to authenticate to ADP company-owned devices, ADP exercises no control over associates' or contractors' choice to use the feature and does not assert any rights to access or control the Biometric Data.

Biometric Data Storage and Security Practices

ADP and/or its vendors shall use a reasonable standard of care and implement appropriate organizational, technical and physical safeguards to store, transmit and protect from loss or unauthorized access, use or disclosure any paper or electronic Biometric Data collected, and shall store, transmit, and protect all Biometric Data in a manner that is the same as or more protective than the manner in which ADP handles and protects other personal information that can

be used to uniquely identify an individual or an individual's account, government issued identification (e.g. Tax ID, Driver's License), financial account data. ADP embeds multiple layers of protection into its products, processes, and infrastructure, to ensure that security remains at the forefront of ADP products and services. For more information on ADP's Data Security at ADP please visit: www.adp.com/about-adp/data-security.aspx.

Cross Border Data Transfers

The biometric data we process may be transferred to any country or region where ADP has operations and elsewhere in the world where our service providers or other entities with whom we share data are located to carry out the above purposes. Any such transfers will be carried out in accordance with applicable law, and appropriate safeguards will be implemented to protect your biometric data. While your biometric data is in another jurisdiction, it may be subject to access requests by courts, law enforcement and national security authorities of that jurisdiction, in accordance with its local laws.

How to Contact Us

For client employees who would like more specific details about how their biometric data is collected and processed, we encourage you to contact your employer directly.

For all other users who have any questions or concerns about this Policy or ADP's information handling practices, please contact us directly at privacy@adp.com.