Always Designing for People®

Effective Date: May 26, 2020

ADP CANADA'S BIOMETRIC INFORMATION PRIVACY STATEMENT

ADP Canada Co. ("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 under applicable federal, provincial and/or territorial laws. **ADP's clients are responsible for developing and complying with their own biometric data handling practices policies as may be required under applicable law.**

Biometric Data Defined

Biometric Data means any biological characteristics of a person, or information based upon such a characteristic or measurements 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 an 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 clients are responsible for compliance with applicable law governing any collection, storage, use, and/or transmission of Biometric Data they conduct or facilitate. To the extent required by law, ADP clients will obtain all required consents (including any written consents where required) from each employee for the client, ADP and/or ADP's authorized licensors or vendors to collect, store, use, and/or transmit Biometric Data prior to the collection of such data.

ADP and/or its vendors also may collect, store, use and/or transmit Biometric Data during the course of conducting ADP's operations and providing products or services to ADP clients and client employees. 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.

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 ADP or to the ADP client.

Disclosure

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

Always Designing for People®

a. First having the client's employee's written consent;

b. The disclosed information completes a financial transaction authorized by the client's employee;

c. Disclosure is required by provincial/territorial or federal law; or

d. Disclosure is required pursuant to law, a valid warrant or subpoena.

Retention Schedule

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.

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 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.

Biometric Data Storage, Security Practices and Cross Border Data Transfers

ADP and/or its vendors shall use a reasonable standard of care to store, transmit and protect from disclosure any paper or electronic Biometric Data collected, and shall store, transmit, and protect from disclosure 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 or property, social insurance numbers, account numbers, PINs, and driver's license numbers. 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.

ADP's use of biometric technologies in its operations or in the delivery of product and services to ADP clients may involve ADP affiliates or subcontractors located in other countries, and ADP may transfer or permit access to Biometric Data for such purposes outside of Canada. As a result, Biometric Data may be subject to applicable local laws, and accessible to the local courts and law enforcement authorities.