Always Designing for People®

ADP U.S. BIOMETRIC INFORMATION PRIVACY POLICY

ADP has instituted the following policy related to 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. **ADP's clients are responsible for developing and complying with their own biometric data retention and destruction policies as may be required under applicable law.**

Biometric Data Defined

As used in this policy, biometric data means any biological characteristics of a person, or information based upon such a characteristic, including characteristics such as those defined as "biometric identifiers" and "biometric information" under the Illinois Biometric Information Privacy Act, 740 ILCS 14/1, *et seq.* "Biometric identifier" means a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry. "Biometric information" means any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual.

Collection, Storage, Use, and Transmission of Biometric Data

ADP clients are responsible for compliance with applicable law governing any collection, storage, use, and/or transmission of biometric data they conduct or facilitate. ADP is requiring all clients to obtain consent-at-the-clock from their employees prior to use of the biometric timekeeping devices, which consent provides authorization for 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 of 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 written authorization from each individual prior to the collection of such 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 services.

Timekeeping Devices and Attachments

ADP clients agree that, in light of the developing nature of the legal requirements that may apply to biometric timekeeping devices, or timekeeping devices attachments, to the extent that such clients use biometric timekeeping devices, or timekeeping devices attachments, they must:

a. Inform the employee in writing that biometric data is being collected, stored, and used;

b. Indicate the specific purpose(s) for collecting biometric data and length of time for which it is being collected, stored, and used; and

c. Receive a written release from the employee (or his or her legally authorized representative) authorizing the client, ADP and/or ADP's authorized licensors or vendors to collect, use, store and transmit employee

biometric data, and authorizing the client to provide such data to ADP and/or ADP's authorized licensors or vendors.

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:

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 state or federal law; or

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

Retention Schedule

ADP will retain any client's employee's biometric data in ADP's possession generated by timekeeping devices or timekeeping devices attachments until the client notifies ADP that it has terminated the employee in the client's timekeeping or HR systems, or has otherwise discontinued using biometric timekeeping devices, or timekeeping devices attachments, with respect to that employee. When ADP receives notification that (1) a client's employee's employment has been terminated; or (2) the client otherwise has discontinued using biometric timekeeping devices, or timekeeping devices attachments, with respect to that employee, any employee's biometric data in ADP's possession will be destroyed.

ADP will retain any client's employee's biometric data in ADP's possession generated by ADP providing other products or services to ADP clients and client employees until the client notifies ADP that it has terminated the employee in the client's timekeeping or HR systems or has discontinued using the applicable ADP products or services, or the client's employee makes a request to ADP that such biometric data be destroyed.

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. Where biometric data is used to authenticate to 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

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 stores, transmits, and protects other personal information that can be used to uniquely identify an individual or an individual's account or property,

such as genetic markers, genetic testing information, account numbers, PINs, driver's license numbers, and social security numbers.