ADP BIOMETRIC INFORMATION PRIVACY POLICY

ADP has instituted the following policy related to the information that is collected and transmitted to ADP as a result of ADP client’s use of biometric timeclocks, or timeclock attachments. **Clients are responsible for maintaining their own data collection, disclosure, retention, and storage policies as may apply to them under applicable law.**

**Biometric Data Defined**

As used in this policy, biometric data includes “biometric identifiers” and “biometric information” as defined in the Illinois Biometric Information Privacy Act, 740 ILCS 14/1, *et seq.*, or as may be defined in any other applicable local laws that govern the collection, use, storage or disclosure of biometric data. “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 of Biometric Data**

ADP clients are responsible for compliance with applicable law and for adopting their own biometric data privacy policies. To the extent required by law, clients will obtain written authorization for the client, ADP, and/or the licensor of ADP time and attendance software to collect, retain, and use biometric data from each employee prior to collection of such data. Biometric data will be used solely for identification, fraud prevention, and pre-employment hiring purposes.

ADP clients agree that, in light of the developing nature of the legal requirements that may apply to biometric timeclocks, or timeclock attachments, to the extent that they use biometric timeclocks or timeclock attachments in jurisdictions where applicable law so requires, 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 the 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) of the biometric data authorizing the client, ADP and/or the licensor of ADP time and attendance software to collect, store, and retain the employee biometric data utilized by the timeclocks, or timeclock attachments, and authorizing the client to provide such data to ADP and the licensor of ADP time and attendance software.

ADP will not sell, lease or trade any biometric data that it receives from its clients as a result of their use of biometric timeclocks, or timeclock attachments.
ADP BIOMETRIC INFORMATION PRIVACY POLICY

Disclosure
ADP will not disclose or disseminate any client’s employee’s biometric data to any person or entity other than the client and the licensor of ADP time and attendance software without/unless:

a. First obtaining 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, federal law or other applicable local law; or

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

Retention Schedule
ADP will retain the client’s employee’s biometric data until the client notifies ADP that it has terminated the employee in the client’s timekeeping or HR systems, or has otherwise discontinued using a biometric timeclocks, or timeclock 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 a biometric timeclocks, or timeclock attachments with respect to that employee, the employee’s biometric data in the possession of ADP will be destroyed.

Biometric Data Storage
ADP 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.