



## PeopleGuru Biometric Information Privacy Policy

In order to comply with laws concerning biometric data, PeopleGuru has instituted the following Policy:

### Biometric Data Defined

As used in this Policy, “biometric data” means “biometric identifiers” and “biometric information”.

### Customer Responsibilities

*Each employer that is using the PeopleGuru Online Service (“Customer”) is responsible for maintaining and setting up within the PeopleGuru Online Service their own data collection, disclosure, retention, and storage policies as may apply to them under the law.*

### Biometric Identifier Defined

“Biometric identifier” means a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry. Biometric identifiers do not include writing samples, written signatures, photographs, human biological samples used for valid scientific testing or screening, demographic data, tattoo descriptions, or physical descriptions such as height, weight, hair color, or eye color.

### Biometric Information Defined

“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. Biometric information does not include information derived from items or procedures excluded under the section Biometric Identifier Defined.

### Collection of Biometric Data

Biometric data will be used solely for identity verification, recording time at work, and other employment-related purposes.

### Disclosure

PeopleGuru will not sell, trade, or otherwise profit from biometric data. PeopleGuru will not disclose or disseminate any biometric data without/unless:

- The employee or the employee’s legally authorized representative has provided written consent to such disclosure or dissemination;
- The disclosed data completes a financial transaction requested or authorized by the employee or the employee’s legally authorized representative;
- Disclosure is required by state or federal law or municipal ordinance; or
- Disclosure is required pursuant to a valid warrant or subpoena

### Data Storage

Once captured biometric Information is converted into an encrypted data string and stored and transmitted securely. PeopleGuru shall use a reasonable standard of care to store, transmit, and protect from disclosure any paper or electronic biometric data collected.



### **PeopleGuru Retention Policy**

PeopleGuru will use a reasonable standard of care to retain active customers' and terminated customers' data according to Customer defined retention system policies within the PeopleGuru Online Service.

#### *Current and Active Employer Data Retention*

Data retention of current and active employer data follows Customer defined retention system policies within the PeopleGuru Online Service. This includes Biometric and personal data, but is not limited to such information. Customer's may choose to modify PeopleGuru Online Services' default retention policies to meet their individual needs:

- Banking records are retained during active employment and up to one-year post employment termination unless otherwise defined by Customer.
- Biometric Identifier records are retained during active employment up to one-year post employment termination unless otherwise defined by Customer.
- Employee HR records are retained five years unless otherwise defined by Customer.
- Payroll records are retained five years unless otherwise defined by Customer.
- Employee and Job Applicant Personal records are retained during active employment and up to three years post-employment termination unless otherwise defined by Customer.

#### *Terminated Customer Data Retention*

For Customers that have terminated the PeopleGuru Online Service, Customer data will be maintained in PeopleGuru Online Service until all governmental filings are complete and for up to one year thereafter. Subsequent to completion of the required governmental filings, Customer data will be moved to an offline status and available for retrieval for five years. In rare cases, PeopleGuru may be required to maintain Customer for periods of time exceeding five years if such data is required to support an active audit, under subpoena by local, state, or the Federal government, or by court order.