Biometric Information Privacy Policy

Sage Hospitality and its managed businesses ("Company") collect certain biometric data from associates. This policy explains what information Sage Hospitality and its managed businesses collect, how this information is used, how it is stored, safeguarded, retained, and disposed of.

Biometric Data Collected by Employer

As used in this policy, "Biometric data" includes "biometric identifiers" and biometric information as "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 identifiers do not include information captured from a patient in a health care setting or information collected, used, or stored for health care treatment, payment, or operations under the federal Health Insurance Portability and Accountability Act of 1996.

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 definition of biometric identifiers.

Purpose for Collection of Biometric Data

The Company, its vendors, and/or the licensor of the Company's time and attendance software collect, store, and use biometric data solely for associate identification, fraud prevention, and pre-employment hiring purposes.

Disclosure and Authorization

To the extent that the Company, its vendors, and/or the licensor of the Company's time and attendance software collect, capture, or otherwise obtain biometric data relating to an associate, the Company must first:

a. Inform the associate in writing that the Company, its vendors, and/or the licensor of the Company's time and attendance software are collecting, capturing, or otherwise obtaining the associate's biometric data, and that the Company is providing such biometric data to its vendors and the licensor of the Company's time and attendance software;
b. Inform the associate in writing of the specific purpose and length of time for which the associate's biometric data is being collected, stored, and used; and

c. Receive a written release signed by the associate (or his or her legally authorized representative) authorizing the Company, its vendors, and/or the licensor of the Company's time and attendance software to collect, store, and use the associate's biometric data for the specific purposes disclosed by the Company, and for the Company to provide such biometric data to its vendors and the licensor of the Company's time and attendance software.

Biometric Information Privacy Policy

The Company, its vendors, and/or the licensor of the Company's time and attendance software will not sell, lease, trade, or otherwise profit from associates' biometric data; provided, however, that the Company's vendors and the licensor of the Company's time and attendance software may be paid for products or services used by the Company that utilize such biometric data.

Privacy of Biometric Data

The Company will not disclose or disseminate any biometric data to anyone other than its vendors and the licensor of the Company's time and attendance software providing products and services using biometric data without/unless:

a. First obtaining written associate consent to such disclosure or dissemination;

b. The disclosed data completes a financial transaction requested or authorized by the associate;

c. Disclosure is required by state or federal law or municipal ordinance; or

d. Disclosure is required pursuant to a valid warrant or subpoena issued by a court of competent jurisdiction.

Retention Schedule

a. Upon termination of employment, biometric data collected is destroyed. This process is conducted on a weekly basis; or

b. Upon company transfer to a location or position where biometric data is no longer needed, such biometric data is destroyed. This process is conducted on weekly basis.

Data Storage

The Company shall use a reasonable standard of care to store, transmit and protect from disclosure any paper or electronic biometric data collected. Such storage, transmission, and protection from disclosure shall be performed in a manner that is the same as or more protective than the manner in which the Company stores, transmits and protects from disclosure other confidential and sensitive information, including 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.