Biometric Data Policy

Policy Criteria:

Brief Policy Description: Provides guidance to ensure the collection, use and management of biometric information is in compliance with the law.
Policy Contact: TrueBlue Legal Compliance
Applies to: TrueBlue and its subsidiaries

Purpose:

This Biometric Data Policy ("Policy") establishes TrueBlue's expectations regarding the use of systems that collect Biometric Data.

Definitions:

Biometric Identifier means an employee's physical or behavioral characteristics. Biometric Data includes DNA; fingerprints; voiceprints; images of the iris, fingerprint, face, hand, palm, vein patterns, and voice recordings from which an identifier template can be extracted; keystroke patterns or rhythms; gait patterns or rhythms; retina or iris scans; and scans of hand or face geometry.
Biometric Information means any information, regardless of how it is captured, converted, stored, or shared, based on an employee's biometric identifier that is used to identify an employee.
Biometric Data means Biometric Identifiers and Biometric Information.

Policy:

Because Biometric Data laws are complex and can vary state to state, TrueBlue prohibits the collection, use, storage, possession, or disclosure of Biometric Data, as well as obtaining Biometric Data through any other means, unless pre-approved, in writing, by the Legal Department. This prohibition applies to the use of client systems in regard to TrueBlue temporary and permanent employees. Permission will be granted on a case-by-case basis, and only if the following criteria are met:

- There are policies and procedures in place that provide for the storage and retention of Biometric Data in accordance with applicable standards and laws including, but not limited to, the Illinois Biometric Information Privacy Act ("BIPA");
- An employee's Biometric Data will not be collected, captured, purchased, received through trade, or otherwise obtained by the Company or our client without prior written consent of the employee;
- The Company or our client will inform employees, in writing, that Biometric Data is being collected or stored and of the purpose and length of term for which their Biometric Data is being collected, stored, and used;
- The Company and our client will not sell, lease, trade, or otherwise profit from an employee's Biometric Data;
- An employee's Biometric Data will not be disclosed, redisclosed, or otherwise disseminated unless (i) consent is obtained from the employee, or (ii) such disclosure or redisclosure completes a pay transaction authorized by the employee, or (iii) such disclosure or redisclosure is required by law or by valid legal subpoena;
- Biometric Data will be stored, transmitted, and protected from disclosure using a reasonable standard of care and in a manner that is the same or exceeds the standards used to store, transmit, and protect other confidential and sensitive information held by the

Company and/or its client;

- The Company and/or its client will permanently destroy Biometric Data it/they possess within a reasonable period of time of when the purpose for obtaining or collecting such data has been fulfilled, but no later than three years, unless and to the extent a shorter time period is required by law, from the Company's last contact with the employee

Questions?

A copy of this document can be found in the Company's internal policy library, and will be made available to the public at www.trueblue.com or upon request. If employees have questions or require additional information on any policy, they should contact their supervisor or management personnel. For all questions relating to this policy or approval to use Biometric Data, please contact iComply@trueblue.com.