Flexential's Biometric Information and Security Policy

Flexential Corp. ("Flexential", "we", or "us") takes measures to ensure its proprietary and confidential information remains private and is committed to maintain an industry leading security system for access to our secure locations within our data centers (collectively "Facility"). The system limits access to such locations to authorized employees, customers, agents, contractors, vendors, and third-party business partners of Flexential ("Authorized Person").

Flexential's security system utilizes certain data that may be considered biometric data under applicable laws for the purpose of authenticating some Authorized Persons' identity and allowing those Authorized Persons access to a Facility or secure location. Flexential has developed and published this policy to provide notice to Authorized Persons and ensure such potentially biometric data is reasonably safeguarded and not retained for longer than necessary. This policy governs the collection, use, retention, and destruction of potentially biometric data and is available to all Flexential employees and the public in the Privacy Notice section on Flexential's website.

This policy is intended to comply with applicable federal, state, and local laws.

Collection and Storage of Potentially Biometric Data.

Among the measures taken by Flexential to protect our secure locations is the use of finger scanning devices, which, along with an Authorized Person's unique badge, authenticates the Authorized Person's identity. We collect finger scan data to enroll you and provide you with biometrically authenticated access.

Depending on the security system in operation at the Facility, the scanning technology measures certain aspects of an Authorized Person's finger or fingers, which are then immediately converted to an encrypted mathematical file (template) based on the distinct characteristics of the finger(s). The template is then securely retained on applications and infrastructure owned and maintained by Flexential. No fingerprints are retained after we create the template.

Before collecting an Authorized Person's finger scan data and creating a template, Flexential obtains a signed consent and written release from the Authorized Person or the Authorized Person's legally authorized representative to obtain and use the finger scan data as outlined in this policy. Flexential will consider requests from an Authorized Person on an individual basis for accommodation or exemption—in whole or in part—from this policy.

Use of Potentially Biometric Data.

Flexential will use the template solely for purposes of authenticating an Authorized Person's identity to access our Facility. The template is compared with the template associated with the Authorized Person's unique badge during the initial enrollment process to verify and authenticate the Authorized Person's identity.

How We Provide Access to Potentially Biometric Data.

Flexential utilizes software and hardware in connection with our security system sourced from third party vendors; however, no third party has access to the templates except as otherwise detailed in this policy. Flexential will not sell, lease, trade or otherwise profit from an Authorized Person's templates. Likewise, Flexential will not disclose, re-disclose or otherwise disseminate templates without an Authorized Person's consent unless required: (1) by any state law, federal law or municipal ordinance; or (2) by valid warrant or valid subpoena issued by a court of competent jurisdiction.

How We Retain, Safeguard, and Destroy Potentially Biometric Data.

Unless otherwise required by law, Flexential will retain an Authorized Person's templates until the earlier of the following occurs:

- When an Authorized Person's Customer Portal profile is removed;
- An Authorized Person's Facility access is removed;
- If the Authorized Person is a Flexential employee, upon termination of employment;
- Twelve months following an Authorized Person's last access to a Facility using biometric data; or
- Upon request to Flexential's Privacy Team from the Authorized Person to permanently destroy the template.

Flexential will permanently destroy an Authorized Person's template upon expiration of the above-outlined time periods.

During the time of retention, Flexential will store and safeguard templates using the reasonable standard of care within the industry, and in a manner equally protective as that in which Flexential stores, transmits, and protects other similar confidential and sensitive data.

How to Contact Us.

If you have questions or concerns about this policy, please contact the site manager or the Privacy Team at privacy@flexential.com.

Updates to this Policy.

Flexential reserves the right to amend this policy at any time for any reason.

If any provision of this policy or any part thereof contravenes any appliable law, or if the operation of any provision is determined by applicable law or otherwise to be unenforceable, then such offending provision or part thereof shall be severed, and the remaining provisions given full force and effect.