

IPM Biometric Data Privacy Policy

1. Introduction

Integrated Project Management Company, Inc. (the "Company," "we," "us," or "our") has adopted this Biometric Data Privacy Policy (this "Policy") to explain, in plain language, how we collect, use, store, keep, share, and destroy Biometric Data (defined below) from our employees and other workforce members in the United States (together, "Workforce Members"). This Policy applies when Biometric Data is collected or used through biometric authentication, meeting transcription, and workforce-collaboration systems (together, the "Biometric Systems") provided by our service providers. Biometric Systems scan an individual's face, finger, hand, or other physical feature for recognition and/or verification. These systems create unique data points and a unique mathematical representation, or algorithm, that is used to identify or verify a person's identity, such as when a person uses their face or fingerprint as an authentication measure to access a restricted area or an electronic device. This Policy has been adopted to comply with the Illinois Biometric Information Privacy Act, 740 ILCS 14 ("BIPA"), and other applicable state biometric privacy statutes.

A copy of this Policy is available on IPM's website. You may also request a copy using the contact information in Section 7 below.

2. Definitions

"Biometric Identifier" means a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry. In simpler terms, it means certain body-based measurements or scans that can be used to recognize or verify a person. Biometric Identifier does 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" means any information, no matter how it is captured, converted, stored, or shared, that is based on a Biometric Identifier and used to identify a person. Biometric Information does not include information that comes from items or procedures excluded from the definition of Biometric Identifier.

"Biometric Data" means Biometric Identifiers and Biometric Information together.

3. Categories of Biometric Data Collected

We may collect, capture, receive, or otherwise obtain the following categories of Biometric Data from Workforce Members through the Biometric Systems:

- **Voiceprints** created from analysis of vocal characteristics, such as pitch, tone, cadence, and timbre, during voluntary usage of voice profile enrollment, voice isolation, or speaker recognition features in Microsoft Teams.

- **Face Geometry Scans** created from (i) voluntary face profile enrollment in Microsoft Teams for use in Teams Rooms, BYOD Rooms, IntelliFrame, and related features, and (ii) enrollment in Windows Hello facial recognition on Company-issued devices when the Workforce Member chooses to use facial recognition to sign in.
- **Fingerprint Scans** created from enrollment in Windows Hello fingerprint authentication on Company-issued devices when the Workforce Member chooses to use fingerprint recognition to sign in.

4. Purpose of Collection, Use, and Processing

Enrollment in any Biometric System is voluntary, and we provide commercially reasonable alternative ways to authenticate, such as a PIN, password, or multi-factor authentication, for any Workforce Member who does not want to enroll. We will not retaliate against, take adverse action against, or otherwise disadvantage any Workforce Member who refuses to enroll in the collection of Biometric Data or who opts out of previous enrollment. If a Workforce Member chooses to use applicable Biometric Systems features, the Biometric Data collected or processed by us through our service providers will be used only for the following purposes:

- Providing secure sign-in and access control for Company-issued devices, systems, applications, and information resources.
- Helping Microsoft Teams and Microsoft 365 Copilot identify who is speaking, create accurate transcripts, prepare meeting recaps, track action items, and provide related productivity and collaboration features for meeting participants.
- Improving the quality, clarity, and accuracy of live captions, meeting recordings, and voice-isolation features used by Workforce Members.
- Maintaining the security and integrity of our information systems and helping prevent unauthorized access.
- Complying with our legal, regulatory, contractual, and audit-related obligations.

We will not use Biometric Data for any purpose other than the purposes described in this Policy. If we start collecting or using Biometric Data for any additional purpose, we will update this Policy and, where required by applicable law, obtain a new written release.

5. Disclosure of Biometric Data

We do not sell, lease, trade, or otherwise profit from Workforce Members' Biometric Data. We, along with applicable service providers, will not disclose, redisclose, or otherwise share Biometric Data unless one of the following applies, subject to applicable law:

- The person whose Biometric Data is involved has consented to the disclosure or redisclosure;

- The disclosure or redisclosure completes a financial transaction requested or authorized by that person;
- The disclosure is needed to establish, exercise, or protect our rights, as allowed by applicable law;
- The disclosure is needed to protect the vital interests of natural persons, as allowed by applicable law;
- The disclosure or redisclosure is required by state or federal law or municipal ordinance; or
- The disclosure is required by a valid warrant or subpoena issued by a court with proper authority.

Biometric Data collected, processed, used, and stored under this Policy may be handled at the same time by us and by third-party service providers that host, operate, or support our Biometric Systems, such as Microsoft Corporation, which provides Microsoft Teams, Microsoft 365 Copilot, and Windows Hello. These service providers are legally required to prevent mishandling of Biometric Data and to maintain reasonable safeguards for Biometric Data.

6. Retention, Storage, and Destruction

We will keep Biometric Data only for as long as needed to fulfill the purpose(s) for which it was collected. In all cases, we will not keep Biometric Data for more than three (3) years after the Workforce Member's last interaction with us. Specifically, Biometric Data will be permanently destroyed and, where applicable, we will ask our service provider(s) to permanently delete it, by the earliest of the following:

- The date when the original purpose for collecting the Biometric Data has been satisfied;
- The date when the Workforce Member deletes their voice or face profile in Microsoft Teams, or opts out of Windows Hello enrollment on their Company-issued device; or
- Within ninety (90) days after the Workforce Member separates from us, including a full wipe or reimaging of Company-issued devices.

Notwithstanding the foregoing, we may retain Biometric Data for longer periods when necessary to comply with applicable law, court order, subpoena, or other legal preservation obligation. Any Biometric Data retained for such purposes will be maintained only for as long as reasonably necessary to satisfy the applicable obligation.

Storage and Security. We store Biometric Data in a manner that is the same as or more protective than the manner in which we store other confidential and sensitive information, using industry-standard encryption in transit and at rest.

7. Contact Information

For more information, or if you have questions about this Biometric Data Privacy Policy, or want to request destruction of your Biometric Data, please contact us:

Mail: Integrated Project Management Company, Inc., Attn: Legal Department, 60 N. Frontage Road, Suite 300, Burr Ridge, IL 60527

Phone: (630) 789-8600

Email: privacy@ipmcinc.com

8. Amendments

We reserve the right to amend this Policy from time to time. Material amendments will be communicated to Workforce Members and made publicly available at the location referenced in Section 1. Where required by applicable law, we will obtain a new written release before making any material change to how we collect or use Biometric Data.