Biometric Data Policy

TABLE OF CONTENTS

1. PURPOSE 2
2. SCOPE 2
3. DEFINITIONS AND ROLES 2
4. COLLECTION, NOTICE, AND CONSENT 3
5. DISCLOSURE OF BIOMETRIC DATA 4
6. RETENTION AND DESTRUCTION 5
7. BIOMETRIC DATA SECURITY AND INCIDENT RESPONSE 6
8. AUTOMATED PROCESSING AND ARTIFICIAL INTELLIGENCE IN THE DRIVER SAFETY PROGRAM 7
9. INDIVIDUAL RIGHTS 8
10. REQUIRED PARTICIPATION AND NON-RETALIATION 8
11. REVIEW 9
12. ATTACHMENTS 9
12.1. ATTACHMENT A ..... **Error! Bookmark not defined.**

This information in this document is the property of America Fujikura Ltd. It is not to be used without express permission of the AFL Legal/Compliance Department. For more information visit http://aflconnects.com/Legal-Compliance/Pages/default.aspx

Biometric Data Policy

1. PURPOSE

America Fujikura, Ltd., together with its affiliates (“AFL” or the “Company”), has adopted this publicly available Biometric Data Policy (this “Policy”) to govern the Company’s collection, use, storage, protection, disclosure, retention, and destruction of Biometric Data.

The Company collects Biometric Data from its employees and other authorized drivers of Company-owned, leased, rented, or otherwise authorized fleet vehicles (each, a “Covered Driver”) in connection with the Company’s driver safety program (the “Driver Safety Program”).

The Company also collects, or may collect, Biometric Data from participating manufacturing and services associates (each, a “Participating Associate”) in connection with a separate, voluntary program through which the Company records approved work activities performed by experienced associates in order to create standardized work instructions, training materials, and other process documentation (the “Assembly Documentation Program”).

The Driver Safety Program and the Assembly Documentation Program are governed by distinct purposes and consent requirements, as well as the applicable retention requirements described in this Policy. Except where this Policy expressly distinguishes between them, a “Covered Person” means a Covered Driver or a Participating Associate, and this Policy applies to Biometric Data collected under both the Driver Safety Program and the Assembly Documentation Program.

Protecting the confidentiality, integrity, and security of Biometric Data is a critical responsibility that must be always taken seriously. Compliance with this Policy is mandatory for all personnel who handle Biometric Data.

2. SCOPE

This Policy applies to all Company employees, agents, and representatives, including any contractor, vendor, or third-party service provider that collects, stores, processes, or otherwise accesses Biometric Data on behalf of the Company (each, a “Third-Party Service Provider”). This Policy applies to all Biometric Data collected, maintained, transmitted, stored, retained, or otherwise used by the Company, regardless of the media on which that information is stored, and regardless of whether it relates to a Covered Person or any other individual.

Any employee, regardless of position or title, who violates any provision of this Policy will be subject to discipline, up to and including termination of employment.

This Policy is binding upon employees of an America Fujikura Ltd. affiliate (“AFL” or the "**Company**"). Consult with the Policy Owner if you have any questions about this Policy.

3. DEFINITIONS AND ROLES

“Biometric Data” means, collectively, all Biometric Identifiers and Biometric Information.

This information in this document is the property of America Fujikura Ltd. It is not to be used without express permission of the AFL Legal/Compliance Department. For more information visit http://aflconnects.com/Legal-Compliance/Pages/default.aspx

"Biometric Identifier" means a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry, and any other data generated by automatic measurements of an individual's biological characteristics that is used to identify a specific individual.

Biometric Identifiers do not include:

- Writing samples and written signatures.
- Photographs.
- Human biological samples used for valid scientific testing or screening.
- Demographic data.
- Tattoo descriptions.
- Physical descriptions, such as height, weight, hair color, or eye color.
- Information captured from a patient in a healthcare setting, or information collected, used, or stored for healthcare treatment, payment, or operations under the Health Insurance Portability and Accountability Act (HIPAA).
- Donated organs, tissues, or parts, or blood or serum stored in connection with organ transplants.
- Biological materials regulated under the Genetic Information Privacy Act.

"Biometric Information" means any information, regardless of how it is captured, converted, stored, or shared, that is based on a Biometric Identifier and used to identify an individual. Biometric Information does not include information derived from items or procedures excluded under the definition of Biometric Identifier.

"Driver Monitoring Consent and Release" means a written authorization, including an electronic signature, executed by a Covered Driver (or the individual's legally authorized representative) that constitutes informed written consent to the collection, storage, use, and disclosure of Biometric Data under the Driver Safety Program as described in this Policy.

"Assembly Documentation Consent" means a voluntary written authorization, including an electronic signature, executed by a Participating Associate (or the individual's legally authorized representative) that constitutes informed written consent to the collection, storage, use, and disclosure of Biometric Data under the Assembly Documentation Program as described in this Policy.

4. COLLECTION, NOTICE, AND CONSENT

Under the Driver Safety Program, the Company and its Third-Party Service Providers collect, store, and use Biometric Data consisting of a scan of face geometry (a "faceprint") derived from images captured by in-vehicle cameras. The Company collects this Biometric Data solely for the purpose of monitoring and improving the safety or security of employees and the public (the "Safety Purpose").

Under the Assembly Documentation Program, the Company and its Third-Party Service Providers capture video recordings of Participating Associates performing approved manufacturing work, together with any scan of face or hand geometry derived from those

This information in this document is the property of America Fujikura Ltd. It is not to be used without express permission of the AFL Legal/Compliance Department. For more information visit http://aflconnects.com/Legal-Compliance/Pages/default.aspx

recordings. The Company collects Biometric Data under the Assembly Documentation Program solely to capture, preserve, and standardize manufacturing best practices and to create work instructions, standard operating procedures, training materials, checklists, and related process documentation (the "Assembly Documentation Purpose"). The Company does not use Biometric Data collected under the Assembly Documentation Program to monitor or evaluate the performance of any individual associate and does not use Biometric Data collected under one program for the purpose of the other.

To the extent a video recording made under the Assembly Documentation Program does not contain Biometric Data—for example, where no scan of face or hand geometry capable of identifying an individual is created or retained—that recording is not governed by this Policy and is instead subject to the Company's separate recording and data-retention policies. Before collecting Biometric Data from any individual, the Company will:

- inform the individual, in writing, that a Biometric Identifier or Biometric Information is being collected and stored;
- inform the individual, in writing, of the specific purpose for which the Biometric Data is being collected, stored, and used, and the length of the term for which it will be collected, stored, and used; and
- obtain the individual's Driver Monitoring Consent and Release (for the Driver Safety Program) or Assembly Documentation Consent (for the Assembly Documentation Program) before collection.

The Company treats Biometric Data as sensitive data and obtains the individual's affirmative written consent before collecting or processing it. Where the Company collects Biometric Data for more than one purpose, the individual must consent separately to each purpose, and consent to one program is not a condition of, and does not imply consent to, the other. The Company will not collect, use, or disclose Biometric Data for any purpose that is not disclosed in this Policy without first obtaining additional consent.

This Policy governs Biometric Data only. Company vehicles equipped with the Driver Safety Program's technology also collect GPS and telematics data, which is not Biometric Data and is governed by the Driver Monitoring Consent and Release and the Company's general data-retention policies rather than by this Policy.

5. DISCLOSURE OF BIOMETRIC DATA

Under the Driver Safety Program, the Company's Third-Party Service Provider will provide the in-vehicle camera devices and host and process Biometric Data on the Company's behalf.

Under the Assembly Documentation Program, the Company's Third-Party Service Provider will provide the recording application and host and process Biometric Data on the Company's behalf.

This information in this document is the property of America Fujikura Ltd. It is not to be used without express permission of the AFL Legal/Compliance Department. For more information visit http://aflconnects.com/Legal-Compliance/Pages/default.aspx

Subject to the individual's consent and a written agreement requiring the applicable Third-Party Service Provider to protect the Biometric Data and prohibiting any further disclosure or use, the Company may disclose Biometric Data to that Third-Party Service Provider solely to facilitate the Safety Purpose or the Assembly Documentation Purpose, as applicable. The Company may also disclose Biometric Data to the Company's insurers and attorneys solely to facilitate the Safety Purpose and the Assembly Documentation Purpose.

The Company will not disclose, redisclose, or otherwise disseminate a Covered Person's Biometric Data unless:

- the individual or the individual's legally authorized representative consents to the disclosure or redisclosure;
- the disclosure completes a financial transaction requested or authorized by the individual or the individual's legally authorized representative;
- the disclosure is required by applicable state or federal law or municipal ordinance; or
- the disclosure is required pursuant to a valid warrant or subpoena issued by a court of competent jurisdiction.

The Company does not, and will not, sell, lease, trade, or otherwise profit from Biometric Data.

6. RETENTION AND DESTRUCTION

This Section establishes the Company's retention schedule and destruction guidelines for all Biometric Data in the Company's possession or under its control, including Biometric Data held by any Third-Party Service Provider on the Company's behalf.

Under both Programs, the Company retains Biometric Data only as long as reasonably necessary to fulfill the Safety Purpose or Assembly Documentation Purpose for which it was collected. The Company will permanently destroy a Covered Person's Biometric Data on the earliest of:

- the date the Safety Purpose or Assembly Documentation Purpose, as applicable, for collecting the Biometric Data has been satisfied;
- thirty (30) days after the individual withdraws consent, or otherwise withdraws from the applicable Program;
- for the Driver Safety Program, thirty (30) days after the individual ceases to be authorized to operate covered vehicles;
- if the Company's annual review of this Policy determines that the storage of Biometric Data is no longer necessary, adequate, or relevant to the Safety Purpose or Assembly Documentation Purpose, as applicable, no later than forty-five (45) days after such determination;
- no later than one (1) year after the end of the individual's employment, engagement, or last interaction with the Company; and

This information in this document is the property of America Fujikura Ltd. It is not to be used without express permission of the AFL Legal/Compliance Department. For more information visit http://aflconnects.com/Legal-Compliance/Pages/default.aspx

- in all events, no later than twenty-four (24) months after the individual's last interaction with the applicable Program.

Video footage that does not contain Biometric Data, GPS and telematics data, and other non-Biometric Data are governed by the Company's separate data-retention policies and are not addressed by this Section. Any Biometric Data embedded in or derived from video footage remains subject to this Section.

The work recordings created under the Assembly Documentation Program, once any Biometric Data in or derived from them has been destroyed, de-identified, or removed, are not Biometric Data and may be retained as Company property in accordance with the Company's separate recording and data-retention policies, regardless of the Participating Associate's employment status.

The Company will destroy Biometric Data in a permanent and irreversible manner, such that it cannot be reconstructed or re-identified, using industry-standard secure-deletion methods for both electronic and any paper records. The Company will require, by written agreement, that each Third-Party Service Provider destroy Biometric Data in the same manner and within the same time periods, and will obtain written confirmation or certification of destruction where reasonably available.

If Biometric Data is subject to a legal obligation to retain the data longer than provided by this Section, such as a valid subpoena or a litigation hold, the Company will retain that Biometric Data only for so long as and to the extent required and will destroy it in accordance with this Section as soon as the obligation expires.

7. BIOMETRIC DATA SECURITY AND INCIDENT RESPONSE

The Company will store, transmit, and protect from disclosure all Biometric Data using the reasonable standard of care within the Company's industry, and in a manner that is the same as or more protective than the manner in which the Company stores, transmits, and protects other confidential and sensitive information. Safeguards include access controls limiting access to personnel with a legitimate business need, encryption in transit and at rest where feasible, and contractual data-protection obligations imposed on Third-Party Service Providers.

The Company maintains and follows the incident-response and breach-notification protocol set out below for any actual or suspected security incident that may compromise Biometric Data (a "Security Incident"). A "Breach" means an unauthorized acquisition of Biometric Data that compromises its security, confidentiality, or integrity. The good-faith acquisition of Biometric Data by an employee or agent of the Company for a legitimate business purpose is not a Breach, provided the Biometric Data is not used for an unrelated purpose or subject to further unauthorized disclosure.

Any employee, agent, or Third-Party Service Provider who discovers or suspects a Security Incident must report it immediately to the Company's privacy contact identified in Section 9. By written agreement, the Company requires each Third-Party Service Provider to notify the Company of any actual or suspected Security Incident affecting Biometric Data without unreasonable delay and cooperate in matters relating to the actual or suspected Security Incident.

This information in this document is the property of America Fujikura Ltd. It is not to be used without express permission of the AFL Legal/Compliance Department. For more information visit http://aflconnects.com/Legal-Compliance/Pages/default.aspx

Upon receiving a report, the Company will promptly take reasonable steps to contain the Security Incident, preserve relevant evidence, and investigate its nature, scope, and cause, including identifying which Covered Persons and what categories of Biometric Data are affected. The Company will determine whether the Security Incident constitutes a Breach that triggers notification obligations under applicable law.

If the Company determines that a Breach has occurred, it will notify each affected Covered Person, at no charge, in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement and any measures necessary to determine the scope of the Breach and to restore the reasonable integrity, security, and confidentiality of the data, and in no event later than thirty (30) days after the Company determines that a Breach occurred. The notice will describe, to the extent known, the nature of the Breach; the categories of Biometric Data involved; the date, estimated date, or estimated date range of the Breach; the steps the Company has taken in response; a telephone number and address the individual may use to contact the Company to inquire about the Breach; the toll-free numbers, addresses, and websites for consumer reporting agencies and the Federal Trade Commission; a statement that the individual can obtain information from the Federal Trade Commission and the credit reporting agencies about fraud alerts and security freezes; and any additional content required by applicable law.

The Company will notify state attorneys general, other state regulators, and consumer reporting agencies to the extent, and within the timeframes, required by applicable state breach-notification law. Without limiting the foregoing, where a Breach is reasonably believed to affect the number of residents of a state that triggers that state's attorney-general-notification requirement, the Company will notify that state's attorney general within the time that state requires with the information that the state requires.

The Company may delay notification if a law-enforcement agency determines and advises the Company that notification would interfere with a criminal investigation and will provide notice no later than thirty (30) days after the agency advises that notification will no longer compromise the investigation.

The Company will document each Security Incident, its investigation, and its response, and will implement corrective measures reasonably designed to prevent a recurrence.

8. AUTOMATED PROCESSING AND ARTIFICIAL INTELLIGENCE IN THE DRIVER SAFETY PROGRAM

Under the Driver Safety Program, the Company and its Third-Party Service Provider use automated processing and artificial intelligence ("AI") to analyze Biometric Data, together with related camera and telematics data, to detect safety-related events. The automated-processing provisions of this Section apply to the Driver Safety Program. The Company does not use AI analysis of Biometric Data collected under the Assembly Documentation Program as a factor in any employment-related decision concerning a Participating Associate.

The results of this automated analysis may be used, together with other information, as a factor in employment-related decisions concerning a Covered Driver, including safety coaching and discipline. A trained Company employee reviews each AI-flagged event before

This information in this document is the property of America Fujikura Ltd. It is not to be used without express permission of the AFL Legal/Compliance Department. For more information visit http://aflconnects.com/Legal-Compliance/Pages/default.aspx

the Company takes any employment action, and the Company does not base an employment decision solely on automated output.

The Company will not use AI in a manner that unlawfully discriminates against any individual on the basis of a protected classification, and the Company periodically reviews, or causes to be reviewed, and tests, or causes to be tested, the technology to guard against algorithmic discrimination.

Where AI is a substantial factor in an employment decision that has a material adverse effect on a Covered Driver, the Company will: (a) notify the individual that AI was used in connection with the decision; (b) provide a plain-language explanation of the principal reason or reasons for the decision; (c) give the individual an opportunity to correct any inaccurate personal data used in making the decision; and (d) give the individual an opportunity to appeal the decision to a qualified human reviewer with the authority to overturn or change the decision and who will consider any information the individual submits in support of the appeal.

9. INDIVIDUAL RIGHTS

A Covered Person may, to the extent provided by applicable law:

- confirm whether the Company is processing the individual's Biometric Data and request access to it;
- request correction of inaccurate personal data;
- withdraw consent to the collection, use, and disclosure of Biometric Data at any time; and
- request that the Company delete the Covered Person's Biometric Data and direct any Third-Party Service Provider to do the same, except where the Company is required or specifically permitted by law to retain it (for example, to comply with a legal obligation or a litigation hold, as described in Section 6).

To exercise these rights, or to raise any question or concern about this Policy, a Covered Person may contact the Company's privacy contact at privacy@aflglobal.com. The Company will not unlawfully discriminate or retaliate against an individual for exercising any right under this Policy.

10. REQUIRED PARTICIPATION AND NON-RETALIATION

Because the Driver Safety Program is used solely for the purpose of monitoring and improving the safety or security of employees and the public, participation in the Driver Safety Program—including enrollment and providing the Driver Monitoring Consent and Release—is a condition of operating Company-owned, leased, rented, or otherwise authorized fleet vehicles. An individual who declines to participate may not be authorized to operate such vehicles, which may affect the individual's continued employment or engagement to the extent operating a Company vehicle is a requirement of the position. Where applicable law requires the Company to offer a non-biometric alternative, the Company will provide a reasonable alternative. The Company will not unlawfully retaliate

This information in this document is the property of America Fujikura Ltd. It is not to be used without express permission of the AFL Legal/Compliance Department. For more information visit http://aflconnects.com/Legal-Compliance/Pages/default.aspx

against any individual for exercising a right expressly provided under this Policy or applicable law.

Participation in the Assembly Documentation Program is voluntary. The Company will not require, as a condition of employment, that a Participating Associate consent to the collection or processing of Biometric Data under the Assembly Documentation Program, will not refuse any benefit or opportunity on the basis of a declination, and will not retaliate against any individual who declines to participate in, or who withdraws from, the Assembly Documentation Program.

11. REVIEW

The Company will review this Policy, including its retention schedule and destruction guidelines, at least annually and whenever material changes occur in applicable law or Company practices, and will update it as laws and Company practices change and to confirm that continued storage of Biometric Data remains necessary, adequate, and relevant to the Safety Purpose or Assembly Documentation Purpose, as applicable.

12. ATTACHMENTS

FRM-15097	Driver Monitoring Consent and Release

This information in this document is the property of America Fujikura Ltd. It is not to be used without express permission of the AFL Legal/Compliance Department. For more information visit http://aflconnects.com/Legal-Compliance/Pages/default.aspx

Revision/Review Tracking:

Revision Number	Date	Nature of Modification	Page/Section Modified	Policy Sponsor	Policy Owner
01	01Dec2026	New Driver Safety Program Fleet Safety AI	New	Larry Pearlman, VP EHSS	Kimberly Grimm

This information in this document is the property of America Fujikura Ltd. It is not to be used without express permission of the AFL Legal/Compliance Department. For more information visit http://aflconnects.com/Legal-Compliance/Pages/default.aspx