Privacy Impact Assessment for:

Geotab Telematics for VIU Fleet Vehicles

Initiative:	Geotab Telematics for VIU Fleet Vehicles
Department or Service Area Name:	Facilities Management & Development

Part 1 – General Information and Overview

1.1 What is the Initiative?

Describe your initiative in enough detail that a reader who knows nothing about your work will understand the purpose of your initiative and who your partners and other stakeholders are. Describe what you're doing, how it works, who is involved and when or how long your initiative runs.

What is the Initiative?
The initiative involves the implementation of Geotab telematics devices across our fleet vehicles to improve operational efficiency, safety, and compliance. These devices collect and transmit real-time vehicle data such as location, speed, engine diagnostics, and driver behavior to a secure cloud-based platform. The purpose is to enable better fleet management, reduce fuel consumption, optimize routes, and support preventive maintenance.

How it works:
Each fleet vehicle is equipped with a Geotab device that connects to the vehicle's onboard diagnostics system. Data is encrypted and transmitted to Geotab's secure servers, where it is accessible through a web-based dashboard. Authorized personnel can monitor performance, generate reports, and set alerts for specific conditions (e.g., harsh braking, idling).

Who is involved:

- **Internal stakeholders:** FMD Management (fleet management).
- **External partners:** Geotab (technology provider), Kal-Tire (installers), Enterprise (device sales and fleet management platform managers).

Duration:
This initiative is ongoing as part of our long-term fleet management strategy. Devices have been installed and will remain active for the life cycle of the vehicles, with periodic reviews for effectiveness and compliance.

1.2. What is the scope of the PIA?

Your initiative might be part of a larger one or might be rolled out in phases. What part of the initiative is covered by this PIA? What is out of scope of this PIA?

This Privacy Impact Assessment (PIA) covers **all activities related to the implementation and ongoing use of Geotab telematics devices within our fleet vehicles**. This includes:

- **Collection, transmission, and storage of telematics data** (e.g., vehicle location, speed, engine diagnostics, and driver behavior).
- **Access and use of data** by internal stakeholders for fleet management, compliance, and operational purposes.
- **Integration with Geotab's cloud-based platform** and any associated data processing by Geotab as a service provider.
- **Security measures and privacy controls** applied to protect personal and operational data.

Out of scope:

- Any other fleet management systems or technologies not related to Geotab.
- Broader organizational initiatives unrelated to telematics or vehicle tracking.
- Personal devices or applications outside the Geotab ecosystem.

1.3. Are there any related Privacy Impact Assessments?

Please indicate if this an update on an existing PIA or an additional module that was not covered in the original PIA.

This is a new PIA.

1.4. What are the data or information elements involved in your initiative?

In the table below, please list all the elements of information or data that you might collect, use, store, disclose or access as part of your initiative. If your initiative involves large quantities of information or datasets, you can list categories or other groupings of personal information in an appendix.

Information Type	Information Collected
Personal Information	• Location of the vehicle (which can be linked to individuals based on who has either been assigned or booked out the vehicles. • Driver behavior data (e.g., speeding, seatbelt usage, harsh braking).
Contact details	• Not collected by Geotab, unless linked through account setup (e.g., name & work email for admin users).
Account information: what info is required to set up an account?	• For administrative users: username, email address, password (encrypted), role permissions. • For vehicle drivers: no account required.
Commercial information	• Vehicle details (VIN, make, model, year), fleet assignment, maintenance records, fuel usage, and trip history.

1.4a. Did you list personal information in question 1.4?

Personal information (PI) is any recorded information about an identifiable individual, other than business contact information. Personal information includes information that can be used to identify an individual through association or reference- see the table below for examples of Personal Information.

Business contact information, in turn, is defined as information to enable an individual at a place of business to be contacted and includes the name, position name or title, as well as business

telephone number, address, email or fax number of the individual. BC FIPPA does not protect business contact information.

Examples of Personal Information	
• Name, age, sex, weight, height • Home address, phone number • Race, ethnic origin, sexual orientation • Medical information • Health history • Number or symbol assigned to the individual • Income, purchases and spending habits • Blood type, DNA code, fingerprints	• Marital or family status • Religion • Education • Financial information • Criminal information • Employment information • Personal views or opinions, except if they are about someone else

- If yes, go to Part 2
- If no, answer question 1.5 and submit questions 1 to 1.5 to pia@viu.ca. You do not need to complete the rest of the PIA template.

1.5. How will you reduce the risk of unintentionally collecting or disclosing personal information?

Some initiatives that do not require personal information are at risk of collecting, using, or disclosing personal information inadvertently, which could result in an information incident.

To minimize the risk of inadvertently collecting or disclosing personal information, the following measures will be implemented:

1. **Data Minimization**
   - Configure Geotab to collect only operational data necessary for fleet management (e.g., vehicle diagnostics, location for routing).
   - Avoid linking telematics data to unnecessary personal identifiers beyond what is required for compliance and safety.
2. **Role-Based Access Controls**
   - Limit access to telematics data to authorized personnel only (e.g., fleet managers).
   - Implement user permissions so that sensitive data (such as driver identity) is only visible to those who need it.
3. **Anonymization Where Possible**
   - Use aggregated or anonymized data for reporting and analytics to reduce exposure of individual driver information.
4. **Clear Policies and Training**
   - Provide staff training on privacy obligations and proper handling of telematics data.
   - Establish internal policies prohibiting the use of data for purposes unrelated to fleet management.

5. **Secure Transmission and Storage**
    - Ensure all data is encrypted in transit and at rest using Geotab's security protocols.
6. **Regular Privacy Audits**
    - Conduct periodic reviews to confirm that no unnecessary personal data is being collected or disclosed.
    - Monitor for potential information incidents.

Part 2 – Collection, Use, and Disclosure

This section will help you identify the legal authority for collecting, using, and disclosing personal information, and confirm that all personal information elements are necessary for the purpose of the initiative.

2.1 Four point "Necessity Test" for the collection, use, and disclosure of Personal Information.

To determine if the Personal Information from your initiative meets the necessity threshold, apply the following four-point test to each element of PI from 1.4 above. Note that each element of PI must meet all four points of the test.

Four point "necessity test" for collecting personal information (OIPC Canada, 2016).

1. The information is rationally connected and demonstrably necessary to an operating program or activity
2. The information is likely to be effective in meeting the objectives of the program or activity
3. There are no other less privacy-invasive ways to effectively achieve the objectives of the program or activity
4. The loss of privacy is proportional to the objectives of the program or activity

Personal Information element	Does it meet all four points of the necessity threshold?	Reasons for keeping or excluding from initiative
Location	Yes	Location data is essential for route optimization, fleet tracking, and ensuring driver safety. It is directly connected to operational objectives and cannot be replaced by a less privacy-invasive method.
Driver behavior	Yes	Monitoring driver behavior (e.g., speeding, harsh braking) is necessary for safety programs, reducing accidents, and improving fuel efficiency. There is no alternative that achieves these objectives without collecting this data.
Driver Name / Employee ID	Yes	Required to associate vehicle usage with authorized personnel for accountability and compliance. Alternatives (e.g., anonymous tracking) would prevent enforcement of safety and operational policies.

2.2 Does your initiative involve the use of Artificial Intelligence (AI)? If so, please fill out Appendix One: GenAI Analysis Questions

No

2.3 Personal Information Flow Diagram and/or Personal Information Flow Table

In the table below, list the personal information from question 1.4. Think about how each element of information flows through your project. Your Privacy Officer can help you figure out whether each step is a collection, use, or disclosure, and whether you have the legal authority for the way you're working with the information. Alternatively, you can attach a flow diagram to this PIA. Add rows as necessary.

	Describe the way personal information moves through your initiative step by step as if you were explaining it to someone who does not know about your initiative.	**(Collection, Use or Disclosure)**	**FIPPA or other legal authority (Privacy Office)**
1.	Geotab device collects vehicle location and driver behavior data from the onboard diagnostics system during trips.	Collection	FIPPA 26(c): Information relates to and is necessary for a program or activity (fleet management and safety).
2.	Data is transmitted securely to Geotab's cloud platform and stored for operational use.	Use, Disclosure	FIPPA 32(a): Use is consistent with the purpose for which it was collected. FIPPA s. 33(2)(d) for the purpose for which the information was obtained
3.	Authorized internal staff (fleet managers) access data through the Geotab dashboard for route optimization, maintenance planning, and safety monitoring.	Use	FIPPA 32(a): Use is consistent with the original purpose.
4.	Data may be disclosed to Geotab (service provider) for system maintenance and troubleshooting under contractual agreements.	Disclosure	FIPPA 33.2(d): Disclosure to a service provider for operational purposes.

2.4 Risk Mitigation Table

Thinking through the information flow, identify where there are risks for privacy incidents or data breaches. For each risk, identify a mitigation strategy, as well as the likelihood of an incident, and level of impact or harm if people's information were breached.

Risk Mitigation Table				
	Risk	**Mitigation Strategy**	**Likelihood**	**Impact/harm**
1	Unauthorized access to telematics data (including driver identity and location).	Implement role-based access controls, strong authentication, and regular access audits.	Low	Low
2	Data breach during transmission to Geotab cloud.	Use end-to-end encryption for all data in transit and verify vendor compliance with security standards.	Low	Low
3	Accidental disclosure of personal data in reports or exports.	Apply data minimization and anonymization for reporting; train staff on privacy best practices.	Medium	Low
4	Over-collection of personal information beyond operational need.	Configure Geotab settings to limit data collection to necessary elements; conduct periodic privacy reviews.	Low	Low
5	Insider misuse of data (e.g., tracking drivers for non-business purposes).	Enforce strict internal policies, monitoring, and disciplinary measures; provide privacy training.	Low	Low

Justification for Low Impact Harm Rating

The personal information collected through Geotab telematics—such as driver name, employee ID, and vehicle location—is directly related to business operations and is already known within the organization for legitimate work purposes. Location data reflects business travel in VIU-owned vehicles, not private activities, and therefore does not reveal sensitive personal details. Additionally, the information is not financial, medical, or otherwise highly confidential. For these reasons, any potential breach would have a low impact on individual privacy and is unlikely to cause significant harm beyond minor inconvenience or operational disruption.

2.5. Collection or Privacy Notice

If you are collecting personal information directly from an individual the information is about, FIPPA requires that you provide a collection notice, also known as a privacy notification.

A collection notice must contain the following elements:

- The legal authority and section under FIPPA under which you are collecting personal information.
- The purpose for which you are collecting the personal information and how it will be used.
- The contact information of an employee or officer at VIU who can answer questions about the collection of personal information.

Contact the privacy office for a collection/privacy notice template.

Suggested privacy notification: **Vancouver Island University (VIU) collects personal information through telematics devices installed in VIU fleet vehicles under the authority of section 26(c) of the** Freedom of Information and Protection of Privacy Act **(FIPPA), which permits public bodies to collect personal information when it is necessary for the purposes of operating a program or activity of the public body.**

The personal information collected may include GPS location data, driving behaviour data, vehicle usage information, and related operational metrics. VIU will use this information for the following purposes:

- To ensure the safe and efficient operation of VIU fleet vehicles;
- To support employee driver safety initiatives;
- To enhance operational planning, compliance, and asset management;
- To investigate incidents involving fleet vehicles where required.

These purposes align with FIPPA's requirement that public bodies collect, use, and disclose only the personal information necessary for program delivery and ensure appropriate protection of that information.

If you have any questions about the collection or use of your personal information, please contact:
privacy.officer@viu.ca

Part 3: Storing Personal Information

3.1. Is any personal information being stored outside of Canada?

If you're storing personal information outside of Canada, identify the sensitivity of the personal information and where and how it will be stored.

Not applicable.

3.1.1. Where is the personal information stored?

Information is being stored in Canada.

3.2. Does your initiative involve sensitive personal information?

Examples of sensitive personal information include personal health information, genetic and biometric data, personal finances, geolocation data, criminal records, counselling records, HR records, payroll records, racial or ethnic origin, sexual orientation, religious, philosophical, or political beliefs, etc.

Yes, the initiative collects geolocation data through telematics devices installed in VIU fleet vehicles. While geolocation is classified as sensitive personal information under privacy legislation, in this case, the data is strictly tied to business operations and reflects vehicle movement during work-related activities only. It does not track individuals outside of their professional duties or in private contexts. Access to this data is restricted to authorized personnel, and it is used solely for operational purposes such as route optimization, safety monitoring, and compliance. These factors significantly reduce the privacy risk associated with collecting geolocation data.

If **yes**, please complete **Part 4**: Assessment for Disclosures of Sensitive Personal Information.

If **no**, skip to **Part 5**: Security of Personal Information

Part 4: Assessment for Disclosures of Sensitive Personal Information

Complete this section if you are disclosing sensitive personal information. You may need help from your organization's Privacy Officer.

4.1. Is the sensitive personal information stored by a service provider?

Yes. Geolocation data collected from VIU fleet vehicles is transmitted to and stored on Geotab's secure cloud infrastructure. Geotab acts as a contracted service provider under VIU's agreement and is responsible for maintaining data security and compliance with applicable privacy legislation. Access to this data is restricted to authorized VIU personnel through the Geotab platform.

If yes, fill out the table below, then go to question 4.3. If no, continue to question 5.

Information about Service Provider

Name of service provider	**Name of cloud infrastructure and/or platform provider(s)**	**Where is the sensitive personal information stored (including backups)?**

Geotab	Geotab uses its own secure cloud platform, which is hosted on Amazon Web Services (AWS) infrastructure.	Data centre in Oakville Ontario.

4.2. Provide details on the disclosure, including where and how the personal information is stored.

Answer this if question 4.1 does not apply. Be specific about where and how the information is being stored.

4.3. Is there a contract that includes privacy-related terms?

If there is a contract with the provider, please describe any privacy-related terms in the contract, or attach the privacy schedule.

See attachment: **Privacy Related Terms in Enterprise Fleet Management Contract**

Part 5: Security of Personal Information

Section 30 of FIPPA imposes a duty on the public body to prevent unauthorized access to Personal Information both internally and with any contracted third parties. As such, we need to make sure that personal information is safely secured in both physical and technical environments. **For each item in this section, please describe the security measures for both the service provider and for VIU internally**.

5.1. Please describe the physical security measures related to the initiative (if applicable).

For example, physical security measures may include: the security environment of vendor's data centres; storing records containing PI in locked storage rooms, offices, and/or filing cabinets with controls over distributions of keys/access; locked workstations that do not permit others to view your screen (including when working remotely, etc.

Physical safeguard	VIU	Third Party
Restricted access to property (e.g. key card access)	☒	☒
Security monitoring building	☒	☒
Locked doors	☒	☒
Locked filing cabinets	☒	☒
Locked workstations	☒	☒

Security cameras/ video surveillance systems	☐	☒
Other:	☐	☐

5.2. Please describe the technical security measures related to the initiative (if applicable).

E.g. Encryption standard for data in transit and data at rest; firewalls, strong passwords; MFA; encrypted documents, etc.

Technical Security Measure	VIU	Third Party
Strong password requirement	☒	☒
Multi-factor authentication (MFA)	☐	☒
Role-based access controls	☒	☒
Encryption in transit	☒	☒
Encryption at rest	☒	☒
Isolation control: Application	☒	☒
Isolation control: Network	☒	☒
Isolation control: Database	☒	☒
Regular Security Vulnerability scan and Penetration Testing	☒	☒
Ongoing Security Awareness Training	☒	☒
Configuration management (CMDB)	☒	☐
Security Log Management and Retention	☒	☒
Security Patch management: Server and End Point	☒	☒
Technical control: perimeter firewalls	☒	☒
Technical control: Web application firewalls	☒	☒
Technical control: Distributed denial of service	☒	☒
Technical control: Intrusion prevention system	☒	☒
Technical control: End Point Detection and Response (EDR)	☒	☒
Information Security Incident Response Plan	☒	☐

5.3 Tracking Access / Access Controls. In this section, you will describe how the unit will minimize the risk of unauthorized access to Personal Information.

5.3.1. FIPPA section 30 requires public bodies to manage access to PI based on the principle of "need to know" – that users may only access information that is necessary to do their job. This is frequently accomplished by assigning role-based access controls (RBAC), and by establishing a security matrix that describes which positions/roles are permitted to access specific types or groups of Personal Information. Access to personal information should only be permitted to those who demonstrate their right of access on the security access chart. Please describe how access controls work in the department, or with this initiative. Describe any access controls and/or ways in which you will limit or restrict unauthorized changes (such as additions or deletions) to personal information.

Access to personal information collected through the Geotab telematics system is strictly limited based on the principle of "need to know." Only two roles within the Facilities department have access to the Geotab platform:

- **Manager of Facilities Services**
- **Director of Facilities Management and Development**

These individuals require access to perform essential fleet management functions, such as monitoring vehicle performance, ensuring driver safety, and planning maintenance. Role-based access controls (RBAC) are enforced through Geotab's platform, which requires secure login credentials and assigns permissions based on user roles. Unauthorized changes (such as additions or deletions of data) are prevented through:

- **System-level restrictions**: Only Geotab administrators can modify system configurations.
- **Audit logs**: All access and changes are logged for accountability.
- **Strong authentication**: Password policies and encryption protect against unauthorized access.

This approach ensures compliance with FIPPA section 30 and minimizes the risk of unauthorized disclosure or alteration of personal information.

5.3.2 How will you know if sensitive personal information is accessed, including access by service providers? This should include a description of what information is available through logs.

Access to sensitive personal information within the Geotab platform is monitored through audit logs and system reporting features. These logs record:
User identity (who accessed the system)
Date and time of access
Actions performed (e.g., viewing, exporting, or modifying data)
Data accessed (specific reports or records)
Only authorized VIU personnel (Manager of Facilities Services and Director of Facilities Management and Development) have platform access, and their activities are logged for accountability. Geotab, as the service provider, also maintains logs for system-level access and troubleshooting under

contractual obligations. These logs are reviewed periodically to detect unauthorized access or unusual activity. Any access by Geotab support staff occurs under strict controls and is documented. https://community.geotab.com/s/article/How-to-find-and-read-the-Audit-Logs?language=en_US

5.4 What controls does the provider have in place to prevent unauthorized access to sensitive personal information?

Describe technical, administrative, and/or policy measures in place to protect PI. If using a cloud-based service provider, include a description of controls in each layer of the stack: software level, platform level, infrastructure level.

Geotab and its cloud infrastructure provider (AWS) implement multiple layers of security controls—technical, administrative, and policy-based—to protect sensitive personal information:

1. **Software Level (Geotab Platform)**
   - **Role-Based Access Control (RBAC):** Access is restricted to authorized VIU personnel based on job function.
   - **Strong Authentication:** Secure login credentials and optional multi-factor authentication.
   - **Audit Logging:** All user activity, including data access and changes, is logged for monitoring and compliance.
   - **Data Encryption:** Sensitive data is encrypted both in transit (TLS 1.2+) and at rest using AES-256.
2. **Platform Level**
   - **Secure APIs:** All integrations use authenticated and encrypted API calls.
   - **Regular Security Patching:** Geotab applies timely updates to mitigate vulnerabilities.
   - **Privacy by Design:** Features such as anonymization and data minimization are built into the platform.
3. **Infrastructure Level (AWS Cloud)**
   - **Physical Security:** AWS data centers have 24/7 surveillance, biometric access controls, and strict visitor policies.
   - **Network Security:** Firewalls, intrusion detection systems, and DDoS protection.
   - **Compliance Certifications:** AWS and Geotab maintain SOC 2, ISO 27001, and other industry-standard certifications.
4. **Administrative and Policy Measures**
   - **Vendor Contractual Safeguards:** Geotab is contractually obligated to comply with FIPPA and VIU's privacy requirements.
   - **Employee Training:** Both VIU and Geotab staff receive privacy and security training.
   - **Incident Response Plan:** Defined procedures for detecting, reporting, and mitigating breaches.

Part 6: Accuracy/Correction/Retention of Personal Information

FIPPA section 28 states that a public body must make every reasonable effort to ensure that an individual's personal information is accurate and complete.

6.1 How is an individual's information updated or corrected?

FIPPA section 29 states that a person can ask you to correct their personal information in your custody or control. If it is not possible to update or correct (for physical, procedural or other reasons) it must be noted on the record. **Please explain how it will be updated or annotated. If personal information will be disclosed to others, how will VIU notify them of the update, correction, or annotation?**

Driver-related personal information in the Geotab system (such as name or employee ID) can be updated by the **Manager of Facilities Services** or **Director of Facilities Management and Development** through the Geotab administrative dashboard. If a correction request is received under FIPPA section 29, the following process will apply:

- **Update or Correction:**
  The administrator will update the record in the Geotab platform to reflect accurate information.
- **Annotation if Update Not Possible:**
  If the correction cannot be made (e.g., historical trip data tied to previous credentials), an annotation will be added to the record noting the correction request and the reason it could not be applied.
- **Notification of Disclosure:**
  If the corrected or annotated information has been disclosed to Geotab or other authorized parties, VIU will notify those parties of the update or annotation to maintain consistency.

This process ensures compliance with FIPPA sections 28 and 29 and maintains the integrity of personal information in our custody.

6.2. Does your initiative use personal information to make decisions that directly affect an individual?

FIPPA requires that public bodies keep personal information for a minimum of one year after it is used to make a decision.

Yes. The initiative uses personal information—such as driver behavior and location data—to make operational decisions that may directly affect an individual. Examples include assigning vehicles, addressing unsafe driving practices, and planning training or corrective actions. In compliance with **FIPPA section 28 and 29**, VIU will retain this personal information for **a minimum of one year after it is used to make a decision** to ensure transparency and allow individuals to request access or corrections. After the retention period, data will be securely deleted or anonymized in accordance with VIU's records management policy and contractual obligations with Geotab.

6.3. Do you have a records management schedule in place?

How long will you keep the personal information collected? Is there a plan in place for retention and deletion? Please also use this question to note how long it will be stored by the service provider (if applicable).

Geotab does not automatically delete data unless a purge is initiated or configured by the customer. By default:

- **Retention Period:**
  Geotab retains telematics data for **at least one year**. In practice, data is often kept for **up to two years** unless a purge is scheduled by the database administrator.
  - If Geotab initiates a purge for system integrity, it guarantees a minimum of **365 days of data** prior to the purge date.
  - Customers can configure longer retention periods or export data for archival using Geotab's API or export tools.
- **Backups:**
  Active databases are backed up nightly, and previous backups are stored in separate physical locations for redundancy.
- **Plan for Retention and Deletion:**
  VIU will retain data for **a minimum of one year after it is used to make a decision**, in compliance with FIPPA section 28 and 29. After this period, data will either be purged automatically based on Geotab's retention settings or exported and securely deleted according to VIU's records management policy.

Part 7 – Personal Information Banks

A personal information bank (PIB) is a collection of personal information searchable by name or unique identifier.

7.1. Will your initiative result in a personal information bank?

This initiative will not result in a Personal Information Bank (PIB). While the Geotab system collects personal information such as driver name and geolocation data, it is not organized or searchable by name or unique identifier for purposes beyond operational fleet management. The data is stored in a way that supports vehicle tracking and maintenance, not as a formal PIB under FIPPA.

If yes, please complete the table below:

Describe the type of information in the bank

Name of main organization involved
Any other ministries, agencies, public bodies or organizations involved
Business contact title and phone number for person responsible for managing the Personal Information Bank

Part 8 – Further Information

8.1. Does the initiative involve systematic disclosures of personal information? If yes, please explain.

No, the initiative does not involve systematic disclosures of personal information. Personal information collected through Geotab (such as driver name and geolocation data) is used internally by authorized VIU personnel for fleet management purposes only. Disclosure to the service provider (Geotab) occurs solely for system hosting and maintenance under contractual agreements and is not routine or systematic beyond what is necessary for platform functionality. There are no regular disclosures to external parties or third-party organizations.

8.2. Will the information collected be used for research or statistical purposes?

No, the information collected through Geotab telematics is not intended for research or statistical purposes. It is used exclusively for operational fleet management, including vehicle maintenance planning, route optimization, and driver safety monitoring. While aggregated data may be reviewed internally for performance reporting or efficiency analysis, it is not used for academic research or external statistical studies.

Part 9 – Summary and Proponent Responsibility

This section is for Privacy Office recommendations as well as any limitations due to privacy concerns.

I have reviewed this PIA and the privacy and security policies of Geotab and I am satisfied that they meet industry standards and have adequate safeguards in place to mitigate any risk of breaching personal information. Further, VIU is collecting minimal personal information necessary - as it relates to work/job duties - for operational efficiency, safety, and compliance purposes.

Part 10: Signatures

This PIA accurately documents the data elements and information flow at the time of signing. If there are any changes to the overall initiative, including to the way personal information is collected, used, stored or disclosed, the program area will engage with their Privacy Office and if necessary, complete a PIA update.

Reviewed by	Privacy Officer
Approved by	Director, Facilities Management and Development
Date:	19-Jan-2026

Privacy Related Terms in Enterprise Fleet Management Contract

VIU does not have a contract directly with Geotab, but rather with Enterprise Fleet Management. Geotab services are provided as a part of the greater fleet management contract with Enterprise. The terms of this contract that are related to privacy and telematics data are included below.

2. Use, Access, Ownership and Storage of Telematics Data. Customer acknowledges that the Telematics Data may be collected, generated and transmitted and that Customer shall be entitled to access, use and disclose such Data in its sole discretion. Customer shall be considered the owner of all such Data. Customer retains ultimate and sole responsibility with regard to (i) the selection of categories of Data and establishment of parameters and criteria Customer wishes to receive through its utilization of a Telematics Device, (ii) the types of reports Customer wishes to receive based on the categories of Data and criteria and parameters Customer has selected, and (iii) the monitoring, usage and disclosure of such Data. By way of example, EFMC may provide Customer a driver safety scorecard based on categories of Data and safety criteria and an overall scoring methodology selected by Customer; EFMC will provide Customer reports strictly based on Customer's criteria and Customer will be solely responsible for interpreting and drawing conclusions from the reports, including whether, based on Customer's criteria, a driver is actually a safe driver or not, and Customer will be solely responsible for deciding what action, if any, should be taken regarding any particular drivers.

EFMC's responsibility to Customer with respect to the Data shall be limited as follows: (i) to arrange for the storage of the Data, which may be stored in EFMC's environment, an EFMC affiliate's environment and/or in an unaffiliated third party subcontractor's environment; (ii) to provide access to the Data to Customer; and (iii) to provide reports to the Customer solely based on categories of Data and parameters identified and selected by Customer.

Customer agrees that EFMC and its parent company and affiliates may:

(A) Collect, access, use and/or disclose the Data for the following purposes: (a) to provide services to Customer; (b) to provide or offer additional products and services to Customer; (c) to check, maintain, diagnose, update or repair Customer's Vehicles; (d) to assist or support Customer with managing its vehicle fleet (e) to comply with any other request from Customer; and/or (f) to disclose the Data to a third party as is necessary to accomplish (a) through (e). If additional services are required, the parties may need to enter into a separate agreement;

(B) Collect, access, use and/or disclose the Data to comply with the request or order of a governmental or law enforcement authority; and

(C) Collect, access, use and/or disclose aggregated and anonymized Data for any purposes.

For clarity, no access and/or use of the Data by EFMC or its parent company or affiliates shall impose on EFMC, its parent company or affiliates any responsibility to monitor the Data or Customer's drivers and/or fleet for any purpose, including without limitation, for safety purposes, and Customer hereby releases and holds harmless EFMC from any liability, claims or damages relating thereto. For purposes hereof, "monitor" means the process of reviewing, checking and/or evaluating the Data, whether over a period of time, as part of a regular review or otherwise.

3. Compliance with Privacy Laws; Notices and Consents. Customer agrees to comply with any and all federal, state and local laws, rules, and regulations pertaining to the collection, storage, protection, sharing and use of, and access to, the Telematics Data ("Laws"). Customer will also (a) provide notice to employees/drivers of a Vehicle equipped with a Telematics Device that such Vehicle is so equipped, resulting in the collection, use, sharing and storage of Data, and that such collection, use, sharing and/or storage may be undertaken by Customer, EFMC or a third party; and (b) obtain driver consent to the collection, use, sharing and storage of such Data as described in this Agreement.

Geotab Product Privacy Notice - 2025 [PUB]

https://docs.google.com/document/d/1R59EP5QvjubKsZmUbnddi-NZd2HIwfS6zIYO3d4-EVk/edit?usp=sharing

Geotab Technical and Organizational Data Security Measures STATEMENT (TOMS)

https://docs.google.com/document/d/1b8F7XB86Z0h8xyD4GF3wH3vzwtdzMhKb-SmhYkz8lGs/edit?usp=sharing