Data Protection Policy

1.0 Purpose

Element Fleet Management Corp. ("**Element Fleet**") is committed to compliance with applicable data protection and privacy laws. This Data Protection Policy applies worldwide to Element Fleet and its subsidiaries (collectively, the "**Element Fleet Group**") and is based on generally accepted, basic principles on data protection, privacy, and security. Ensuring data protection is the foundation of trustworthy business relationships and the reputation of the Element Fleet Group as an attractive partner and employer. The purpose of this Data Protection Policy is to ensure that the Element Fleet Group: (a) complies with all applicable federal, state, provincial, territorial and local data protection, privacy, and security laws (collectively, "**Data Protection Laws**") and best practices in the jurisdictions in which it operates; (b) protects the rights of customers, partners and employees; and (c) protects itself from the risk of a data breach.

2.0 Scope

This Data Protection Policy applies to all companies of the Element Fleet Group. The Data Protection Policy extends to all processing of personal data (as defined herein and by Data Protection Laws). In countries where the data of legal entities is protected to the same extent as personal data, this Data Protection Policy applies equally to data of legal entities. Anonymized Data (as defined herein and by Data Protection Laws) is not subject to this Data Protection Policy.

Individual companies of the Element Fleet Group are not entitled to adopt policies or practices that deviate from this Data Protection Policy. If required by Data Protection Laws, additional data protection policies can be created with the prior written consent of the General Counsel.

3.0 Application of Local Laws

This Data Protection Policy is in addition to, and does not replace, Data Protection Laws and is meant to supplement the local data privacy laws of the jurisdictions in which the companies of the Element Fleet Group operate. The Element Fleet Group must comply with all Data Protection Laws and in the event that there is any conflict between applicable Data Protection Laws and this Data Protection Policy, the Data Protection Laws will take precedence. The Element Fleet Group must also comply with the reporting requirements for data processing under applicable local laws.

Each company of the Element Fleet Group is responsible for compliance with this Data Protection Policy and Data Protection Laws related to privacy and data protection. If there is reason to believe that any legal obligations contradict any provisions of this Data Protection Policy, the relevant company must immediately inform both the Chief Technology Officer and General Counsel. In the event of conflicts between Data Protection Laws and this Data Protection Policy, Element Fleet will work with the applicable company of the Element Fleet Group to find a practical solution that complies with Data Protection Laws and meets the overarching purpose of this Data Protection Policy.

4.0 Principles for Processing Personal Data

4.1 Lawfulness

Personal data must at all times be processed in a legal manner that is consistent with the principles described in Element Fleet's external privacy policies, Acceptable Use Policy and Data Classification & Handling Standard, as applicable.

4.2 Restriction to a specific purpose

Personal data can be processed only for the purpose(s) that was defined at the time the data was collected from the Individual.

4.3 Transparency

The Individual must be informed of how their data is being handled. When the data is collected, the Individual must either be aware of, or be informed of:

a) the purpose(s) of data processing;
b) any third parties or categories of third parties to whom the data might be transmitted; and
c) whether their personal data is being transferred outside of the jurisdiction in which they are domiciled.

All Individuals must be provided with, made aware of, or directed to, Element Fleet's applicable external privacy policies.

4.4 Data reduction and data economy

Before processing personal data, it must be determined whether and to what extent the processing of personal data is necessary in order to achieve the purpose for which it is undertaken. Anonymized Data should be used when reasonably practicable. Personal data should not be collected in advance and stored for potential future or undefined purposes unless required or permitted by applicable Data Protection Laws.

4.5 Deletion

Personal data that no longer serves a legitimate business or legal purpose must be deleted in accordance with applicable data retention policies or anonymized in a manner permitted by applicable Data Protection Laws.

4.6 Factual accuracy of data

Reasonable steps must be taken to ensure that if the Element Fleet Group becomes aware of any personal data that is inaccurate or incomplete, such personal data is deleted, corrected, supplemented or updated. Where a request is made by an Individual to correct or complete their personal data, it should be dealt with in a timely manner. If there are any issues with respect to the request, they should be immediately brought to the attention of the Element Fleet Group's General Counsel and Chief Technology Officer.

4.7 Confidentiality and data security

Personal data must be treated as confidential and secured with appropriate administrative, physical and technical measures to prevent unauthorized access, illegal processing or distribution, as well as accidental loss, modification or destruction. Personal data should only be accessed by personnel who require the

information in the course of their employment duties. Please refer to Element Fleet's Disclosure Policy and Data Classification and Handling Standard for the steps that must be taken to protect confidential information.

4.8 Privacy by design

When new processes or product offerings are being developed, or changes to existing processes are expected, whereby personal data will be processed, the principles of data protection set out in this Data Protection Policy will be considered. The General Counsel and Chief Technology Officer must approve any material changes to the type of personal data that is collected or the way in which personal data is processed.

5.0 Purposes for Data Processing

Collecting, processing and using personal data is permitted under the following circumstances.

5.1 Customer, driver and partner data

5.1.1 Data processing for a contractual relationship

Personal data of prospects, customers, drivers and partners can be processed in order to establish, execute, perform or terminate a contract. This also includes any services to be provided in connection with the contract. Prior to the execution of a contract – during the contract initiation phase – personal data can be processed to prepare proposals or for other matters that relate to the negotiation and execution of the contract. Prospects can be contacted during the contract negotiation process using the information that they have provided. Any restrictions requested by the prospects must be complied with. Personal data of drivers may be collected from the customer (i.e., the drivers' employer) or directly from the drivers.

5.1.2 Data processing for customer loyalty or advertising purposes

If the Individual contacts an Element Fleet Group company to request information (e.g. request to receive informational materials about a product), data processing to meet this request is permitted.

Customer loyalty or advertising measures are subject to additional requirements. Personal data can be processed for customer loyalty initiatives or targeted advertising purposes provided that this is consistent with this Policy. The Individual must be informed about the use of their data for customer loyalty or advertising purposes and that providing data for this purpose is voluntary. When communicating with the Individual, consent shall be obtained from him/her to process the data for customer loyalty or advertising purposes where required by law. The Individual's decision to provide consent must be documented at the time it is obtained. When giving consent, the Individual should be given a choice among available forms of contact such as regular mail, e-mail and phone.

If the Individual refuses the use of their data for customer loyalty or advertising purposes, it can no longer be used for these purposes and must be blocked from use for these purposes. Any other legal restrictions in specific jurisdictions regarding the use of data for customer loyalty or advertising purposes must be observed.

5.1.3 Consent to data processing

Where legally required, consent from the Individual must be obtained before personal data can be processed. The declaration of consent must be obtained in writing or electronically for the purposes of documentation. In some circumstances, such as telephone conversations, consent can be given verbally. The granting of consent must be documented. If personal data regarding drivers is provided to the

Element Fleet Group by a customer (i.e., the drivers' employer), consent from such drivers can be assumed provided that the customer confirms that it has obtained the drivers' consent to the processing of such personal data. If personal data regarding a driver is obtained directly by the Element Fleet Group (i.e., through an application in the driver's vehicles), consent to the processing of such personal data must be obtained directly from the driver.

5.1.4 Data processing pursuant to applicable laws

In limited instances, the processing of personal data is also permitted in absence of consent from the individual, if permitted by Data Protection Laws. The type and extent of data processing must be necessary for the legally required data processing activity and must comply with Data Protection Laws. To the extent members of the Element Fleet Group intend to rely on such exceptions, they must seek prior approval from the General Counsel.

5.1.5 Data processing pursuant to legitimate interest

Personal data can also be processed if it is necessary for a legitimate interest of the Element Fleet Group. Legitimate interests are generally of a legal (e.g. litigation or collection of outstanding receivables) or commercial nature (e.g. avoiding breaches of contract).

5.1.6 Processing of highly sensitive personal data

Highly sensitive personal data (as defined herein) can be processed only if required to perform obligations under contract, if required by law or if it is necessary for asserting, exercising or defending legal claims of the Element Fleet Group regarding the Individual. If there are plans to process highly sensitive personal data, the General Counsel and Chief Technology Officer must be informed in advance.

5.1.7 User data and internet

If personal data is collected, processed and used on websites or in apps, Individuals must be informed of this in a privacy statement. Individuals must also be informed through a privacy statement and/or website footer if their use of a website or app is monitored or tracked for targeted advertising purposes. Personal tracking may only be completed if it is permitted by Data Protection Laws.

5.2 **Employee data**

5.2.1 Consent to data processing

Where legally required, consent from the employee must be obtained before personal data can be processed. Such consent must be obtained in writing or electronically. In certain circumstances, consent may be given verbally, in which case it must be properly documented. In the event of informed, voluntary provision of data by the relevant party, consent can be assumed if Data Protection Laws do not require express consent.

5.2.2 Data processing pursuant to applicable laws

In limited instances, the processing of personal employee data is also permitted in absence of consent from the individual, if permitted by Data Protection Laws. The type and extent of data processing must be necessary for the legally authorized data processing activity and must comply with Data Protection Laws. To the extent members of the Element Fleet Group intend to rely on such exceptions, they must seek prior approval from the General Counsel.

5.2.3 Collective agreements on data processing

Data processing may also be permitted if authorized through a collective agreement. The agreement must cover the specific purpose of the intended data processing activity and the data processing activity must comply with Data Protection Laws.

5.2.4 Data processing pursuant to legitimate interest

Personal data can also be processed if it is necessary for a legitimate interest of the Element Fleet Group.

5.2.5 Processing of highly sensitive data

Highly sensitive personal data can be processed only if required by law or if it is necessary for asserting, exercising or defending legal claims of the Element Fleet Group regarding the Individual. If there are plans to process highly sensitive personal data, the Chief Technology Officer must be informed in advance in writing.

5.2.6 Telecommunications and internet

Telephone equipment, e-mail addresses, intranet and internet along with internal social networks are provided by the Element Fleet Group primarily for work-related assignments. They are a tool and a company resource. They can be used in accordance with applicable laws and internal company policies. There will be no general monitoring of telephone and e-mail communications or intranet/ internet use. To defend against attacks on the IT infrastructure of the Element Fleet Group or on individual users, protective measures can be implemented for the connections to the Element Fleet Group networks that block technically harmful content or that analyze the attack patterns. For security reasons, the use of telephone equipment, e-mail addresses, the intranet/internet and internal social networks can be logged for a temporary period. Evaluations of this data from a specific person can be made only in a concrete, justified case of suspected violations of laws or policies of the Element Fleet Group.

6.0 Transmission of Personal Data to Third Parties

Any transmission of personal data to a third party must be completed in a manner that is consistent with the requirements set out in Element Fleet's external privacy policies, Acceptable Use Policy and Data Classification & Handling Standard. In addition, such personal data must be used by the third party solely in furtherance of the purpose for which it was collected. If there is uncertainty about whether a transmission of personal data to a third party is appropriate and complies with the above requirements, the General Counsel should be consulted.

In the event that personal data is transmitted to a third party outside the Element Fleet Group, unless such transmission is required by applicable law, the third party should provide a representation or other assurance that it complies with Data Protection Laws and/or the Element Fleet Group should take reasonable steps to confirm that such third party complies with Data Protection Laws. If appropriate, a third party data security assessment should be completed before personal data is transmitted to third parties.

If data is transmitted by a third party to the Element Fleet Group, such data must be used solely for its intended purpose and must be protected in accordance with this Data Protection Policy.

7.0 Contract Data Processing

If the Element Fleet Group engages a third party to provide data processing services, the following requirements must be complied with:

a) the service provider must confirm that it adheres to applicable Data Protection Laws;

b) the service provider must be selected based on, among other things, its ability to comply with the data protection measures in this Data Protection Policy;

c) the Element Fleet Group must provide written instructions on data processing and the responsibilities of Element Fleet Group and the service provider must be documented; and

d) the Element Fleet Group must take reasonable steps to confirm that the service provider will comply with the requirements of Data Protection Laws and such steps should be repeated on a regular basis during the term of the data processing contract.

8.0 Rights of the Individual

Every Individual has the following rights:

a) the Individual may request information on which personal data relating to him/her has been stored, how the data was collected, and for what purpose;

b) if personal data is incorrect or incomplete, the Individual can demand that it be corrected or supplemented;

c) the Individual can object to the processing of their data for purposes of customer loyalty, advertising or market research. The data must be blocked from these types of use;

d) the individual can request delivery of their personal data; and

e) the individual can request deletion of their personal data.

Element Fleet's external privacy policies shall provide contact information where requests can be made related to the collection, use and disclosure of personal data.

9.0 Confidentiality of Processing

Personal data should be safeguarded. Any unauthorized collection, processing, or use of such data by employees is prohibited.

Employees are strictly forbidden to use personal data for private or commercial purposes, to disclose it to unauthorized persons, or to make it available in any other way outside of their employment duties. All employees must be informed about their obligation to protect personal data and this obligation shall remain in force after their employment has ended with Element Fleet Group. All employees shall be required to read this Data Protection Policy as well as Element Fleet's Disclosure Policy which contains additional requirements about the protection of confidential information and their responsibilities thereunder.

10.0 Processing Security

Personal data must be safeguarded from unauthorized access and unlawful processing or disclosure, as well as accidental loss, modification or destruction. This applies regardless of whether data is processed electronically or in paper form.

11.0 Compliance, Data Protection Controls and Governance

Compliance with this Data Protection Policy and Data Protection Laws should be monitored regularly with data protection audits and other controls. The performance of these controls is the responsibility of the General Counsel, Chief Technology Officer, Chief Financial Officer or other company units with audit rights and/or external auditors. The General Counsel and Chief Technology Officer, or such other appropriate person as they determine, will periodically report to the Board of Directors of Element Fleet (the "**Board**") on the Element Fleet Group's compliance with this Data Protection Policy and Data Protection Laws. The Board will consider whether the Element Fleet Group's policies and procedures with respect to data protection are adequate and whether any changes are required.

12.0 Risk Management

The General Counsel, Chief Technology Officer and Chief Financial Officer are responsible for assessing the risks faced by the Element Fleet Group with respect to data protection and privacy. Risks shall be defined and measured as the result of threat probability multiplied by the potential impact. Risks that could affect the Element Fleet Group shall be assessed and monitored on a periodic basis, as appropriate. Risk Assessments will be performed to assist in the identification of existing and emerging threats and vulnerabilities, measurement of risk, and selection of appropriate risk mitigation strategies at least annually. A risk assessment should also be initiated whenever:

a) there are significant changes to the type of personal data that is collected by the Element Fleet Group or the manner in which such personal data is processed;

b) non-compliance with the Element Fleet Group's policies or procedures with respect to data protection has been identified, its business impact is considered significant, and it cannot be mitigated within a reasonable timeframe;

c) a critical vulnerability has been reported or otherwise identified and cannot be eliminated within a reasonable timeframe;

d) a risk assessment has been requested following an audit; or

e) the management believes that there is a reason to request such an assessment.

13.0 Data Protection Incidents

All employees must inform their supervisor immediately about potential violations of this Data Protection Policy or applicable Data Protection Laws, including unauthorized access to personal data or loss of personal data (a "**Data Protection Incident**"). Such supervisor must inform both the Chief Technology Officer and General Counsel immediately about the Data Protection Incident.
In the event of a Data Protection Incident, such as:

a) improper use of personal data by an Element Fleet employee;

b) improper transmission of personal data to third parties;

c) improper access by third parties to personal data; or

d) loss of personal data,

the Chief Technology Officer and General Counsel must ensure that the Element Fleet Group complies with its reporting obligations under Data Protection Laws. The Chief Technology Officer will, in consultation with the General Counsel and other members of the Element Fleet Group's senior management team, determine an appropriate course of action in response to a Data Protection Incident. A record about all Data Protection Incidents will be kept in compliance with applicable Data Protection Laws. All responses to Data Protection Incidents must also comply with Element Fleet's Data Incident Response Policy.

14.0 Responsibilities and Sanctions

The General Counsel and Chief Technology Officer is responsible for ensuring that all measures are in place so that any data processing is carried out in accordance with this Data Protection Policy. Compliance with the Data Protection Policy is the responsibility of all employees of the Element Fleet Group and all employees must acknowledge in writing or electronically that they have read, understand and agree to comply with this Data Protection Policy. Improper processing of personal data, or other violations of Data Protection Laws can be criminally prosecuted in many jurisdictions and may result in claims for compensation of damage. Violations for which individual employees are responsible can lead to disciplinary action, including termination of employment, and to sanctions under applicable law.

15.0 Training

Any employee that handles personal data during the course of their employment should receive the necessary training to ensure that they comply with the Element Fleet Group's policies and procedures with respect to data protection. Element Fleet will periodically conduct security awareness training for employees.

16.0 Amendments to Data Protection Policy

Any amendments to this Data Protection Policy shall be subject to approval by the General Counsel and Chief Technology Officer.

17.0 Definitions

a) "Anonymized Data" means information that cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular Individual, provided that a business that uses Anonymized Data: (i) has implemented technical safeguards that prohibit reidentification of the consumer to whom the information may pertain; (ii) has implemented business processes that specifically prohibit reidentification of the information; (iii) has implemented business processes to prevent inadvertent release of deidentified information; and (iv) makes no attempt to reidentify the information.

b) "Individual" means any natural person whose data can be processed. In some countries, legal entities can be individuals as well.

c) "Highly sensitive personal data" is data about racial and ethnic origin, religion, union membership or the health and sexual life of the Individual, genetic or biometric data, social security/insurance number, or medical information. Under Data

d) Protection Laws, further data categories can be considered highly sensitive.

e) "Personal data" is any information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular individual.

f) “Processing of personal data” means any process to collect, store, organize, retain, modify, query, use, forward, transmit, disseminate or combine and compare data. This also includes disposing of, deleting and blocking data and data storage media.

18.0 Contact

Any questions or concerns regarding this Data Protection Policy should be addressed to:
Chris Gittens
Chief Digital Officer
Element Fleet Management Corp.
161 Bay Street, Suite 3600
Toronto, ON M5J 2S1
cgittens@elementcorp.com

or

David Colman
General Counsel
Element Fleet Management Corp.
161 Bay Street, Suite 3600
Toronto, ON M5J 2S1
dcolman@elementcorp.com

Administration

These guidelines are administered by the Chief Digital Officer and General Counsel. They are regularly reviewed and may be updated at any time.

Version #	Description	Author	Policy Approver(s)	Effective Date
1.1	Original Version	Legal	General Counsel and Chief Technology Officer	May 7, 2019
1.2	General updates	Legal	General Counsel and Chief Technology Officer	September 1, 2020
1.3	General updates	Legal	General Counsel and Chief Digital Officer	November 1, 2021
1.4	General updates	Legal	Data Governance Council	April 11, 2022