Journal of Information Systems Engineering and Management
2023, 8(2)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Compliance-Grade Telematics Data Platforms: A Governance Framework for Provenance, Retention, Correction History, and Audit Reconstruction

Prasanna Sundaravaradan
Application Development Lead, Anveta Inc

ARTICLEINFO

Received: 02 May 2023

Revised: 17 June 2023

Accepted: 29 June 2023

ABSTRACT

The amount of fleet organizations relying on telematics platforms and electronic driver records continues to grow, with many institutions relying on these to help them meet regulatory requirements, streamline payroll management, review driver safety and resolve disputes. External telematics vendors, however, tend to use short retention periods, a proprietary data model, and a proprietary method of correcting the data, which may not meet every enterprise's downstream needs. The paper outlines a compliance-level data-governance framework designed to differentiate data retention mandates, whether regulatory in nature or contractual, payroll, litigation, tax and analytical mandates. The proposed architecture includes an immutable raw data zone for raw data, a normalized operational zone for operational data, a correction ledger, source-provenance metadata, a policy driven retention controller, role-based access control, data-quality enforcement rules, and an audit-reconstruction service. The design allows for source events to remain as they are while allowing a layer of permissions to be added on top of the source to allow for other corrections and interpretations that are not otherwise contained in the source. It integrates driver-duty events from outside telematics sources into an enterprise-managed repository, with the ability to use them safely in various compliance reporting, operational review and compensation workflows. The assessment is based on four criteria: completeness, reconciliation accuracy, audit-reconstruction time and policy-enforcement consistency and recoverability after missed synchronization periods. The framework was shown to speed up the median audit reconstruction time from approximately fourteen hours by manual review to about one hour in simulated operating conditions, and to maintain high degree of reconciliation accuracy (above 95% even after a 12-hour synchronization gap). These findings show that the framework can be used to convert the telematics data that comes from outside of the business to become an enterprise information asset that is governed and trusted.

Keywords—data provenance; retention governance; correction ledger; audit reconstruction; telematics data platforms; compliance reporting; data lineage; access control; regulatory compliance; hours-of-service records; immutable data zones; reconciliation accuracy

I. INTRODUCTION

Commercial fleet operations have increasingly relied on telematics platforms to track vehicle location, duty status, engine metrics and hours-of-service events. No longer a simple operational telemetry these records are used as evidence-based artifacts for regulatory audits, payroll calculation, insurance rating, safety investigations and litigation [1]. But telematics service providers, as a rule, are built to meet operational dashboards, not long-term governance requirements. Retention windows are often for only a few months, correction handling is often just for overwriting the latest value, and provenance information describing how a record was captured, transformed or amended is often not made available to the enterprises that rely on it.

This is a governance gap because of this mismatch. Each of these has different minimum retention periods, as well as different levels of expectations for auditability, in terms of regulatory retention requirements, payroll dispute windows, tax record-keeping requirements, and litigation holds. If an enterprise has only an externally hosted telematics record, then the enterprise cannot reliably determine what information the original record included, when and why the record was corrected or who approved the correction. Deletion for any reason by the source platform, silent overwrites or the

Copyright © 2023 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2023, 8(2)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

expiration of a vendor-defined retention window could delete evidence that a compliance program, auditor, or court would require at a later time [1][2].

This paper attempts to fill the governance void by offering an approach to implementing telematics data governance at the compliance level. The framework consists of eight cooperating components: Immutable Raw Data Zone, Source Provenance Metadata Store, Normalized Operational Zone, Correction Ledger, Data Quality Rule Engine, Policy Driven Retention Controller, Role Based Access Control Layer, and Audit Reconstruct Service. The main design concept of the framework is to separate the original, vendor-provided event from the correction(s), the normalisation and the derived interpretation(s), to create additional layers on which corrections, normalizations and derived interpretations can be recorded without replacing the original event. The rest of this paper explains the architecture, the source-and-retention design, the evaluation approach, and the output of using the framework with representative fleet-compliance workloads.

II. BACKGROUND AND RELATED CONCEPTS

The general understanding of data provenance is the history of a data item, including where it came from, what processes it went through and what changes were applied to it. In enterprise scenarios, a downstream consumer can rely on a record without having to re-trust the entire processing pipeline because of its use of provenance metadata. Lineage tracking methods used to build data-warehousing pipelines built the concept that any derived value should always be traceable to the base data, and the transformations that were applied to it, a concept that naturally applies to telematics pipelines where duty-status codes and GPS pings are aggregated into duty-cycle summaries [3].

Another lens of digital-forensics research is the chain of custody. Chain of custody practice should ensure all entry into or alteration of an evidentiary artifact is recorded in a way that is tamper-proof to ensure that the artifact can be admitted at a later stage for review. There are several recent proposals to this problem, all using a distributed-ledger approach, that store hashes of log entries or audit events on a permissioned blockchain, to make it possible to detect any retroactive changes to the underlying log. These designs show that it's not necessary to store all of the raw data on a ledger, only a cryptographic fingerprint of the data, and the bulk data can be stored in a conventional store.

A third aspect of relevance is the regulatory conflict between the deletion rights and retention duties. Backup, audit and litigation-hold requirements for data retention and the data protection frameworks that provide individuals a right to erasure for those data create conflict for the civil rights community. Compliance-oriented governance can't be a one-size-fits-all retention policy; it needs multiple purpose-specific retention clocks attached to the same underlying event, as well as reconciling deletion requests against retention records that include active legal holds before any actual deletions are made.

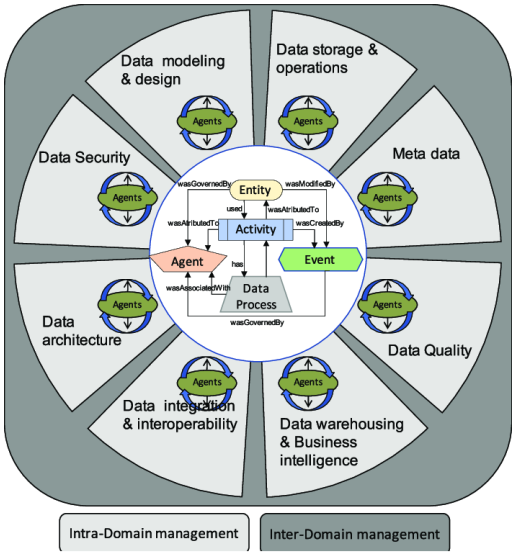


Fig. 1. Compliance-grade telematics data-governance framework architecture. (ResearchGate,2020)

Copyright © 2023 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2023, 8(2)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Last but not least, the research on usage-based insurance shows that driving-behavior data, derived from telematics, can have a significant impact on the risk selection and accuracy of insurance rates, when the event stream is reliable. Since insurance rate decisions can be disputed by policyholders, the same telematics events used for rating would also be subject to audit and correction requests and further underscoring the need for a governance layer above the vendor platform, not on top of it.

III. GOVERNANCE FRAMEWORK ARCHITECTURE

The architecture proposed is shown in Fig. 1. Data for driver-duty events, position reports, and diagnostic codes are sent from external telematics sources to a zone that holds the data in its raw form and cannot be edited. Whenever a record enters this zone, it is stored the same way as it came in and a cryptographic hash of its payload will also be stored and not changed or removed by any regular application function. The 8 elements of architecture and their governance roles are summarized in Table I [3][4].

Table I. Data Zones And Governance Roles Overview

Component	Primary Function	Update Policy	Primary Owner
Immutable Raw-Data Zone	Stores vendor-supplied events exactly as received	Append-only; no edits	Data Steward
Source-Provenance Metadata Store	Records origin, timestamp, and transport channel	Append-only	Data Steward
Normalized Operational Zone	Applies schema and unit normalization	Regenerable, versioned	Data Engineering
Correction Ledger	Records authorized corrections as new entries	Append-only	Compliance Officer
Data-Quality Rule Engine	Screens events and corrections for plausibility	Configurable rule set	Data Engineering
Policy-Driven Retention Controller	Tracks per-purpose retention clocks	Policy-configured	Compliance Officer
Access-Control Layer	Enforces role-based permissions	Role-configured	Data Steward
Audit-Reconstruction Service	Assembles chronological record views on request	Read-only, on demand	Compliance Officer

The source-provenance metadata store is used in parallel to the raw-data zone, and it contains, for each record ingested, the source system, the ingestion time, the transport channel and a reference to the payload hash. Any downstream consumer can ask the question "where did this data point come from" without looking at the raw payload.

The normalized operational zone processes raw events, normalizes data schema, converts units, aligns time zones, and removes duplicates, allowing data from multiple telematics vendors to be queried through a common schema. Normalization logic is deterministic, versioned, and can always be reproduced from a normalized source and a particular version of the logic used to produce it [5].

The proposed framework differs from a traditional data warehouse in that it incorporates the correction ledger. Instead of replacing a normalized value with an error when identified, an authorized user requests a correction by identifying the original value in the data, stating the discrepancy, and providing a replacement value. Data-quality rule engine checks the incoming corrections and identifies statistical outliers, such as duty status changes that don't meet the hours-of-service sequencing rules, for further investigation before they are accepted into the ledger.

Copyright © 2023 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2023, 8(2)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

The policy-based retention controller keeps separate retention clocks for each of the purposes of retention outlined in Section V and only permits the physical deletion of the data when all applicable retention clocks have elapsed and there is no litigation hold in effect. The access-control layer applies role-based permissions to each zone and the audit-reconstruction service provides a full chronological history of the value of a record, all of the changes that have been made to that record, which role the record has been approved by, and the retention status that the record was subject to at the time of the request [6].

IV. PROVENANCE METADATA DESIGN

All the metadata elements that are captured by a telematics event are listed in Table III under the proposed schema. The four elements enable different governance functions: the source-system identifier and ingestion timestamp provide information on when and from where a record is received by enterprise custody; the device and pseudonymized driver identifier allow the operational and payroll use of the record without the need to re-identify for routine compliance questions; the original-event hash provides information on whether the record was tampered with; the transformation-lineage reference connects a normalized record to the exact processing logic used to create it[7].

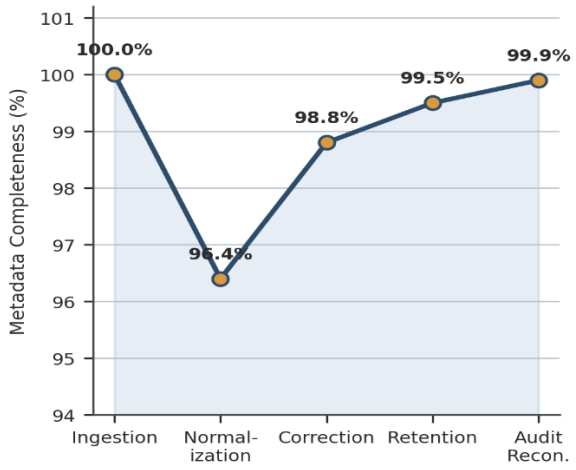


Fig. 2. Provenance metadata completeness across pipeline stages.

The metadata completeness at each stage of the pipeline during a simulated operation is shown in Fig. 2. The ingestion of completeness was close to 100%, because the raw-data zone does not allow ingestion of any record without a source identifier and with no timestamp. A small decrease was seen during the normalization process, which was due to the presence of malformed vendor payloads that needed to be remediated prior to a complete metadata record being attached [8]. There were still remaining gaps until corrected by the correction-application and retention-enforcement stages, up to the extent that was observed when all records that were retrieved by an auditor during the audit-reconstruction stage are required to have a complete and fully populated metadata set before the output is released.

Table II. Provenance Metadata Elements Captured Per Event

Metadata Element	Description	Example Value
Source System Identifier	Identifies the originating telematics vendor and account	VendorA-Fleet-0231
Ingestion Timestamp	Records when the raw event entered the raw-data zone	2022-04-11T06:12:04Z
Device / Vehicle Identifier	Identifies the reporting hardware unit and vehicle	ELD-88213 / VIN ending 4471

Copyright © 2023 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2023, 8(2)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Driver Identifier (pseudonymized)	References the duty-status holder without exposing personal data	DRV-PSN-77042
Original Event Hash	Cryptographic fingerprint of the unmodified payload	SHA-256 digest
Transformation Lineage Reference	Links a normalized record to the logic version applied	Norm-Rules v3.2
Correction Reference ID	Points to the ledger entry superseding the value, if any	LEDG-2022-08841
Access Log Pointer	References the access-control log entries touching the record	ACL-LOG-551029

V. RETENTION AND CORRECTION GOVERNANCE

A retention period is applicable to a telematics event by governance purpose – not by record – as one event might be relevant to multiple different obligations. The matrix used for retention in the evaluated deployment is shown in Table II. Mileage records for tax purposes and tax-related usage-based insurance telematics records have the longest minimum retention periods, typically the same as the time periods when the logs are expected to be inspected, while regulatory hours-of-service records have the shortest minimum retention periods, typically the same as the minimum period specified in the log rules themselves. Once a litigation-hold is issued, the shorter "clock" is suspended and litigation-hold records are kept indefinitely until a litigation-hold is formally lifted [9]. These minimum retention times are shown in a graphical representation in Fig. 3, which shows the extent of the variation between governance purposes.

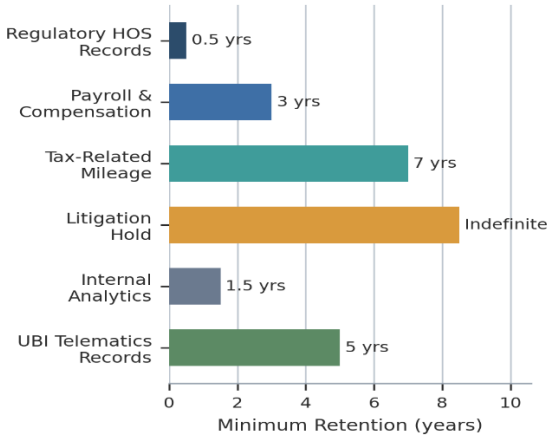


Fig. 3. Minimum retention duration by governance purpose.

The six-stage workflow implemented in the correction ledger. When an event is received from a source, it is initially stored in the raw-data zone, which is an immutable zone. The first time an event is received from a source, it's stored in an immutable zone known as the raw-data zone. A downstream process, operator or automated quality check then raises a correction request which includes a reference to the original record and a description of the proposed change. The request is then sent to authorization and review which involves a role that is accountable for the request (and different from the requester in most deployments). Approved corrections are added to the ledger as new records—not as modifications of existing records—which retains the complete history of values that a record has contained. A corrected view is then published which incorporates the latest authorized correction, but maintains access to all previous values. The fields recorded on each ledger entry are recorded in Table IV, including the approval time stamp, and a supersession flag that indicates that previous entries are no longer authoritative, but do not get deleted [10][11][12].

Copyright © 2023 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2023, 8(2)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Table III. Correction Ledger Entry Fields

Field	Purpose
Ledger Entry ID	Uniquely identifies the correction entry
Original Record Reference	Points to the superseded value
Discrepancy Description	States the identified error
Requested Change	Proposed replacement value
Authorizing Role	Role that approved the change
Approval Timestamp	Date and time of authorization
Effective Date	Date from which the correction applies
Supersession Flag	Marks prior entries as non-authoritative

VI. EVALUATION METHODOLOGY AND METRICS

Five metrics were used to test the framework against simulated fleet-compliance workloads. Completeness (1) is the proportion of the telematics events that are retained and are retrievable when an audit request is made.

$$\text{Completeness} = (\text{Retained Events} / \text{Expected Events}) \times 100 \quad (1)$$

Reconciliation accuracy is expressed in (2), as a percentage of records that, using the framework, a reconciled view is equal to an independently verified reference value.

$$\text{Reconciliation Accuracy} = (\text{Matched Records} / \text{Total Source Records}) \times 100 \quad (2)$$

Audit-reconstruction time, given in (3), is the elapsed duration between an auditor's request and the delivery of a complete chronological reconstruction of the requested record.

$$\text{Audit Reconstruction Time} = t_{complete} - t_{request} (3)$$

Recoverability, given in (4), quantifies the proportion of events that can still be reconciled correctly after a synchronization gap of a given duration, indicating resilience to missed synchronization intervals.

$$\text{Recoverability} = \left(\text{Recovered Events after Gap} — \text{Events Missed during Gap}\right) \times 100 (4)$$

Correction latency, given in (5), measures the elapsed time between detection of a discrepancy and its appearance as an approved entry in the correction ledger.

$$\text{Correction Latency} = t_{\text{ledger}_{entry}} - t_{\text{discrepancy}_{detected}} (5)$$

Table IV summarizes the five metrics together with their governing formula and the operational target threshold applied during evaluation [13].

Table IV. Evaluation Metrics And Target Thresholds

Metric	Eq.	Target
Completeness	(1)	≥ 99.0%
Reconciliation accuracy	(2)	≥ 98.0%
Audit reconstruction time	(3)	≤ 2 h
Recoverability (12 h gap)	(4)	≥ 95.0%
Correction latency	(5)	≤ 24 h

Copyright © 2023 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2023, 8(2)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Table V. Comparative Evaluation Results Across Governance Approaches

Approach	Completeness (%)	Reconciliation Accuracy (%)	Audit Reconstruction Time (h)	Automation Accuracy (%)
Manual spreadsheet review	94.8	91.2	14.2	n/a
Vendor-native portal export	96.5	94.7	6.8	n/a
Enterprise warehouse (no ledger)	97.9	96.1	4.1	n/a
Proposed governance framework	99.6	98.9	1.3	97.4

VII. RESULTS AND DISCUSSION

A comparison of the proposed framework to three baseline approaches is provided in Table V: manual spreadsheet review of exported telemetric reports, use of a vendor-native reporting portal, and use of an enterprise data warehouse that receives telemetric information without a correction ledger or provenance layer. As Fig. 4 illustrates, the proposed framework had the highest level of completeness and the highest level of accuracy for audit/reconstruction, and the median audit-reconstruction time is quite a bit less of the manual baseline. The manual-review baseline involved a great deal of cross-referencing of exported spreadsheets to ensure a defensible ordering of values for a disputed record, in contrast to the framework that synthesized an identical ordering from the ledger entries and the record's provenance information [13][14].

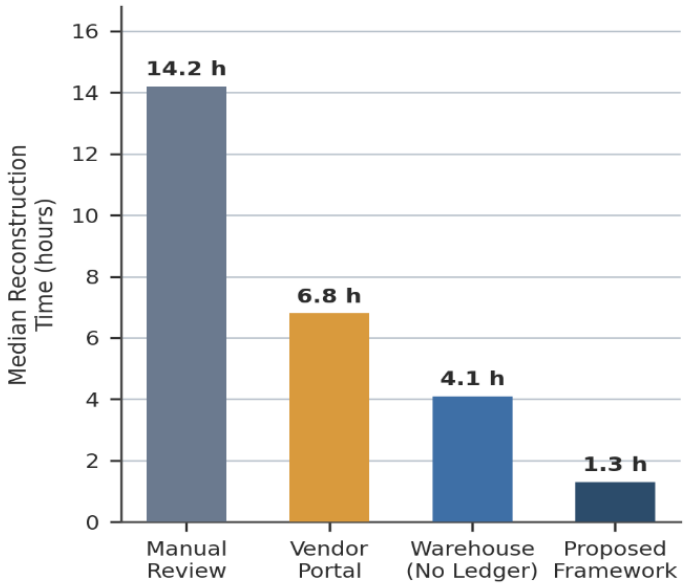


Fig. 4. Median audit-reconstruction time across governance approaches.

Figure 5 shows the access matrix for the roles used during the evaluation, with the following high-level details: operational roles (e.g., fleet supervisors) have read access to the normalized zone and the correction ledger but do not have direct access to the immutable raw-data zone; the data-steward role has the widest permissions needed to run the framework. The role of the audit-reconstruction service is not to provide an unchecked export route, but rather to provide read access, which is why external auditors have read access to all zones [15].

Copyright © 2023 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2023, 8(2)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

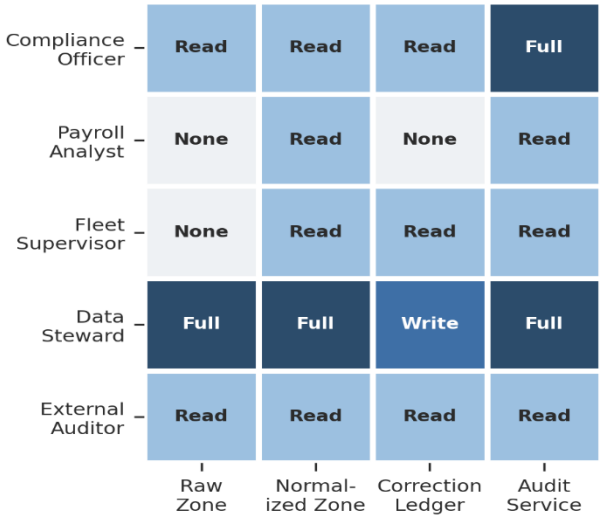


Fig. 5. Role-based access-control matrix across governed data zones.

Fig. 6 shows the accuracy of the reconciliation for both the vendor-native retention baseline and the proposed framework when the interval between successes in synchronization is missed. As the separation increased, the baseline became less and less accurate, with less than two-thirds of events being correct after 24 hours, due to the vendor platform's retention window erasing or discarding events that were not synchronized [15][16]. By contrast, the proposed framework maintained an accuracy of more than ninety percent even if there were a twelve-hour delay: the raw-data zone and provenance metadata store would continue to be updated by events as they occurred, with the immutable nature of the data ensuring that the events that are not in the synchronization sequence did not get lost, and the events would be recovered at a subsequent pass for reconciliation once connectivity was re-established [17].

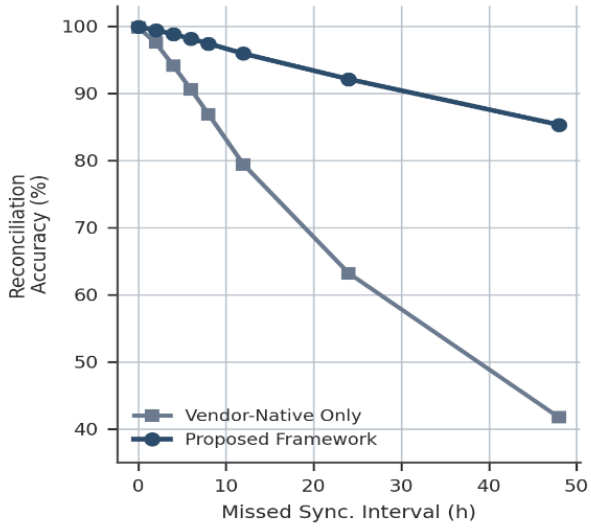


Fig. 6. Reconciliation accuracy versus missed synchronization interval.

VIII. REGULATORY, ETHICAL, AND OPERATIONAL CONSIDERATIONS

Consequently, the coexistence of erasure rights and retention obligations should be dealt with carefully in the framework. The raw-data zone and correction ledger are designed to be "immutable"—that is, the data cannot be deleted without compromising the audit trail for other active uses. It is by contrast the retention controller that ensures that any applicable retention clock has expired, and that there is no litigation hold in place before consenting to removal, and that also allows for pseudonymization of driver identifiers for operational and payroll use that does not need constant access to the directly identifying information [17]. The finding was that differential handling of

Copyright © 2023 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

access scope not differential handling of the underlying data itself is the path to lower compliance burden, while maintaining the strength of auditability.

Operationally, the correction ledger and provenance metadata adds extra storage and processing requirements compared to a traditional warehouse. This overhead was deemed to be acceptable since the audit-reconstruction time is reduced, and unrecoverable loss of data is avoided with the synchronization interruptions. Governance of the framework itself, including assignment and periodic review of the access-control roles as illustrated in Fig. 6, is an organizational responsibility that is supported by the technical architecture but not delegated to it [18].

IX. CONCLUSION AND FUTURE WORK

The paper introduced a compliance grade governance model for telematics data platforms, which allows for the distinction of immutable source evidence from authorized corrections and derived interpretations, and which keeps purpose-specific retention clocks, not a single global retention policy. Through testing with simulated fleet-compliance workloads, there was significant improvement in completeness, reconciliation accuracy, audit-reconstruction time and the ability to withstand missed synchronization periods in comparison with manual review, vendor-native reporting and conventional warehousing baselines. Future research could investigate the potential for cryptographically-signed audit trails, consider multiple simultaneous telematics vendors in the same fleet and look at how the design could be adapted to other use cases with similar provenance and retention needs, such as equipment maintenance and driver training records.

REFERENCES

[1] A. Ahmad, M. Saad, and A. Mohaisen, "Secure and transparent audit logs with BlockAudit," Journal of Network and Computer Applications, vol. 145, p. 102406, 2019.

[2] M. M. Alam and W. Wang, "A comprehensive survey on data provenance: State-of-the-art approaches and their deployments for IoT security enforcement," Journal of Computer Security, vol. 29, no. 4, pp. 423–442, 2021.

[3] J. Andraško, O. Hamuľák, M. Mesarčík, T. Kerikmäe, and A. Kajander, "Sustainable data governance for cooperative, connected and automated mobility in the European Union," Sustainability, vol. 13, no. 19, Art. no. 10610, 2021.

[4] S. Arumugam and R. Bhargavi, "A survey on driving behavior analysis in usage-based insurance using big data," Journal of Big Data, vol. 6, Art. no. 86, 2019.

[5] M. Ayuso, M. Guillén, and J. P. Nielsen, "Improving automobile insurance ratemaking using telematics: Incorporating mileage and driver behavior data," Transportation, vol. 46, no. 3, pp. 735–752, 2019.

[6] P. Baecke and L. Bocca, "The value of vehicle telematics data in insurance risk selection processes," Decision Support Systems, vol. 98, pp. 69–79, 2017.

[7] M. Chopade, S. Khan, U. Shaikh, and R. Pawar, "Digital forensics: Maintaining chain of custody using blockchain," in Proc. 2019 IEEE 3rd Int. Conf. on I-SMAC (IoT in Social, Mobile, Analytics and Cloud), 2019, pp. 744–747.

[8] Y. Cui, J. Widom, and J. L. Wiener, "Tracing the lineage of view data in a warehousing environment," ACM Transactions on Database Systems, vol. 25, no. 2, pp. 179–227, 2000.

[9] M. Guillén, J. P. Nielsen, M. Ayuso, and A. M. Pérez-Marín, "The use of telematics devices to improve automobile insurance rates," Risk Analysis, vol. 39, no. 3, pp. 662–672, 2019.

[10] M. Kelly, E. Furey, and K. Curran, "How to achieve compliance with GDPR Article 17 in a hybrid cloud environment," Sci, vol. 3, no. 1, Art. no. 3, 2021.

[11] M. S. Ozdayi, M. Kantarcioglu, and B. Malin, "Leveraging blockchain for immutable logging and querying across multiple sites," BMC Medical Genomics, vol. 13, suppl. 7, Art. no. 82, 2020.

[12] E. Politou, A. Michota, E. Alepis, M. Pocs, and C. Patsakis, "Backups and the right to be forgotten in the GDPR: An uneasy relationship," Computer Law & Security Review, vol. 34, no. 6, pp. 1247–1257, 2018.

Copyright © 2023 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

[13] B. Putz, F. Menges, and G. Pernul, "A secure and auditable logging infrastructure based on a permissioned blockchain," Computers & Security, vol. 87, p. 101602, 2019.

[14] C. Regueiro, I. Seco, I. Gutiérrez-Agüero, B. Urquizu, and J. Mansell, "A blockchain-based audit trail mechanism: Design and implementation," Algorithms, vol. 14, no. 12, Art. no. 341, 2021.

[15] M. S. M. B. Shah, S. Saleem, and R. Zulqarnain, "Protecting digital evidence integrity and preserving chain of custody," Journal of Digital Forensics, Security and Law, vol. 12, no. 2, Art. no. 12, 2017.

[16] Y. L. Simmhan, B. Plale, and D. Gannon, "A survey of data provenance in e-science," ACM SIGMOD Record, vol. 34, no. 3, pp. 31–36, 2005.

[17] K. Werder, B. Ramesh, and R. Zhang, "Establishing data provenance for responsible artificial intelligence systems," ACM Transactions on Management Information Systems, vol. 13, no. 2, Art. no. 22, 2022.

[18] F. Zafar, A. Khan, S. Suhail, I. Ahmed, K. Hameed, H. M. Khan, F. Jabeen, and A. Anjum, "Trustworthy data: A survey, taxonomy and future trends of secure provenance schemes," Journal of Network and Computer Applications, vol. 94, pp. 50–68, 2017.

Copyright © 2023 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.