Group Data Retention Policy

Version 1.1
24 March 2026

1. Introduction

The Summit Automotive Group is committed to complying with the law and regulations in all our business activities, including applicable Data Protection Laws.

We are committed to using all appropriate technical and organisational measures to ensure the protection of both customer and employee personal data.

This policy, and the associated policies, set out the expected behaviours of our employees, contractors and third parties in relation to the retention, storage destruction of all data held within the business (including personal data). This policy should be read in conjunction with our Group Data Protection policy.

Any references to 'Summit Automotive', 'we', 'our' and 'us' refers to all subsidiaries in The Summit Automotive Group.

2. Scope

Maintaining business data in a systematic and reliable manner is essential to comply with our legal and regulatory requirements. It also reduces the costs and risks associated with retaining unnecessary information.

A vital part of our Data Protection Policy and practice is that personal data is retained for the appropriate period of time, neither too long nor too short. It is paramount that the retention period allows us to meet our legal and regulatory requirements but that the rights of data subjects are also protected.

This policy has been developed to help employees properly manage personal data in a consistent manner. It sets out:

- How long personal data should be retained
- How records should be disposed of

Unless otherwise stipulated, the policy refers to both hard copy and electronic documents. This document should be read in conjunction with our Data Protection Policy.

3. Definitions

Personal Data: Any information (including opinions and intentions) which relates to an identified or identifiable natural person.

Identifiable natural person: Anyone who can be identified, directly or indirectly, in particular by reference to an identifier such as name, and identification number, location data, an online identifier, or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Data Controller: A natural or legal person, Public Authority, Agency or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.

Data Subject: The identified or identifiable natural person to which the data refers.

Process, processed, processing: Any operation or set of operations performed on Personal Data or on sets of Personal Data, whether or not by automated means. Operations performed may include collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Data Protection: The process of safeguarding Personal Data from unauthorised or unlawful disclosure, access, alteration, Processing, transfer or destruction.

Data Protection Authority: An independent Public Authority responsible for monitoring the application of the relevant Data Protection regulations – in the UK this is the ICO.

Data Processors: A natural or legal Person, Public Authority, Agency or other body which Processes Personal Data on behalf of a Data Controller.

Consent: Any freely given, specific, informed and unambiguous indication of the Data Subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the Processing of Personal Data relating to him or her.

Special Categories of Data: Personal Data pertaining to or revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, data concerning health or sex life and sexual orientation, genetic data or biometric data.

Third Country: Any country not recognised as having an adequate level of legal protection for the rights and freedoms of Data Subjects in relation to the Processing of Personal Data.

Profiling: Any form of automated processing of Personal Data where Personal Data is used to evaluate specific or general characteristics relating to an identifiable natural person.

Personal Data Breach: A breach of security leading to the accidental or unlawful; destruction, loss, alteration, unauthorised disclosure of, of access to, Personal Data transmitted, stored or otherwise Processed.

Encryption: The process of converting information or data into code, to prevent unauthorised access.

Pseudonymisation: Data amended in such a way that no individuals can be identified from the data (whether directly or indirectly) without a key that allows the data to be re-identified.

Anonymisation: Data amended in such a way that no individuals can be identified from the data (whether directly or indirectly) by any means or by any person.

GDPR: The General Data Protection Regulation

4. Roles and Responsibilities

All employees, including contractors and third parties who process data on our behalf are responsible for complying with the requirements of this policy.

The Data Protection and Legal Compliance Manager is responsible for maintaining the policy and monitoring compliance.

All Department Heads are responsible for ensuring that documented procedures are in place to comply with the requirements of this policy.

It is the responsibility of all employees to ensure that they have read the most up to date version of this policy which will be available on our website.

5. Policy

Information/records (hard copy and electronic) will be retained for at least the period specified in our Data Retention Guidelines (see Appendix 1).

Hard copy and electronically held records, documents and information must be deleted at the end of the retention period.

5.1 Suspending the destruction date

If a claim, audit, investigation, subpoena, or litigation has been asserted or filed by or against us, or is reasonably foreseeable, we have an obligation to retain all relevant records, including those that otherwise would be scheduled for destruction under the records retention schedule.

5.2 How long should we keep our data?

Data should be kept for as long as it is needed to meet the terms of our agreement with our customers and any applicable legal requirements. Our Group Data Retention Guidelines (below) have been agreed following an assessment of our data and the requirements of all our Regulators, together with our obligations under Data Protection Laws.

5.3 Methods of Destruction

All data, whether hard copy or electronic should be destroyed in a secure manner, preserving the confidentiality of all personal data.

All hard copy data must be disposed of in the confidential waste bins which are located in every area of the business. Under no circumstances should confidential or personal data be put into normal waste bins. We will maintain records of the secure destruction of all waste which is put into the confidential waste.

Our IT department will ensure that all electronic data is securely destroyed in a way which cannot be restored. They will also be responsible for ensuring that any electronic equipment is securely wiped, and where appropriate securely disposed of, when it is no longer required by the business.

5.4 Sharing of Information

Duplicate information should be destroyed. Where information has been regularly shared between business areas care should be taken to ensure that all copies of the data are destroyed in line with the Data Retention Guidelines.

6. Training

All employees will have their responsibilities under this policy outlined to them as part of their induction training. All employees will complete an annual refresher of this training. We will provide further training and guidance if there are any updates made to this policy and/or the associated policies and procedures.

7. Monitoring Compliance

As a minimum the following will be monitored to ensure compliance with this policy:

- An annual Data Protection Compliance Audit which will, at the minimum assess:
  - Compliance with policy in relation to the protection of personal data, including:
    - Correct storage of personal data
    - Deletion of personal data in accordance with the schedule

Key business stakeholders will devise a plan with a schedule for correcting any identified deficiencies within a defined and reasonable time frame. Any major deficiencies identified will be reported to and monitored by the Data Protection and Legal Compliance Manager.

8. Review

This policy is owned by the Data Protection and Legal Compliance Manager and will be reviewed at least annually. We will provide information and/or training on any changes we make.

9. Related Documents

- Group Data Protection Policy
- Group Data Retention Guidelines

Schedule 1 – Group Data Retention Guidelines

Client Personal Data

Each claim which we process generates a number of documents throughout the claims cycle. Some of these documents are able to be deleted immediately after use or at a certain stage throughout the claim. Other documents need to be retained for future reference or in respect of hire and repair invoices they need to be kept for 6 years to satisfy financial accounting requirements. All of these documents are currently kept in a storage folder called "Client Files" and are accessed through the front-end KAM database.

In respect of the management of these documents, our system is able to categorize each document and subsequently treat them accordingly as follows:

Day One Deletion

Documents that fall into this category are initial claim forms either submitted by a work partner or similar documents which KAM generate which are then sent to insurers for information purposes. These will contain personal data relating to our own client as well as other third parties involved in the accident.

48-Hour Deletion

These documents will predominantly those generated by our system and will be scheduled to be processed and sent overnight to work partners and insurers. Again these will include full claim data for reporting purposes. After 48 hours from creation these are then automatically deleted.

Other Claim Documents

There will be a number of other documents that are generated throughout the claims cycle which are not deemed to be of significant risk but which are required for the smooth running of the claim.

Closed Files

Once a claim is closed all documents contained within the "Client File" folder are moved to a new storage folder named "Closed Files". Access can still be gained to these documents through the KAM database for a period of 6 months in case of any subsequent queries post settlement. After 6 months the documents will be moved again to a secure storage area with no day to day access. All data held to satisfy financial accounting requirements for the 6-year period is then anonymised in its entirety.

Backups

Machine Images (snapshots) – weekly backup retained for 12 months, a monthly backup is retained for 24 months. Full details are provided in our Backup Policy.

Call Recordings

Summit Automotive records all incoming telephone calls for training and monitoring purposes excluding any card data. These are retained for a period of 3 years before deletion.

Our Authorised Legal Counsel/Representatives

Our authorised legal counsel/representatives will retain client files electronically for 6 years post conclusion of the client matter, after which time they will be securely deleted.

Central business records

Record type	Retention period
Accounts/Financial Records	6 years
Company Records including Directors details	6 years from the end of the last company financial year they relate to
Complaints records	6 years
Records relating to matters where a potential claim or legal case has been notified to the business	6 years

HR records

Employers are required by law to keep certain records relating to their workers and their business for specified periods. The table below sets out the requirements.

Employment law

Drivers' hours, work breaks and rest breaks

Record: Tachograph record cards designed to record drivers' hours, work breaks and rest breaks.

Retention period: Minimum of one year after use.

National minimum wage

Record: Records sufficient to establish that every worker is being, or has been, remunerated at a rate at least equal to the national minimum wage.

Retention period: Three years from the day the pay reference period immediately following that to which the records relate ends.

Working time restrictions

Record: Records that are adequate to show that the limits on weekly working time, daily and weekly working time for young workers, and night work are being met.

Retention period: Two years from the date on which the records were made.

Incapacity for work and statutory sick pay

Record: All sickness periods lasting at least four days; statutory sick pay (SSP) payments; and weeks SSP not paid and why.

Retention period: Three years after the end of the tax year in which the sickness periods occurred and SSP payments were made.

Absence during pregnancy and statutory maternity pay

Record: Details of absence from work due to pregnancy, statutory maternity pay (SMP) weeks and amounts, and any medical certificate relating to expected week of confinement.

Retention period: Three years after the end of the tax year in which the employee's maternity pay period ended.

Statutory paternity pay, statutory shared parental pay and statutory adoption pay

Record: Details of paternity pay period, evidence of entitlement, payment weeks and amounts, and any unpaid weeks within the pay period.

Retention period: Three years after the end of the tax year in which payments were made.

Health and safety legislation

Accidents at work and work-related illness

Record: Every employer with 10 or more employees must keep readily accessible a means by which an employee may record the particulars of any accident causing personal injury.

Retention period: Minimum of three years from the date on which the record was made.

Injuries, fatalities, diseases and dangerous occurrences

Record: Record of any reportable incident under the Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 2013.

Retention period: Minimum of three years from the date on which the record was made.

Inspection of excavations, cofferdams or caissons

Record: Report of inspection by a competent person of excavations, cofferdams or caissons.

Retention period: Until the excavation, cofferdam or caisson is complete and after that for three months.

Obtaining lifting equipment

Record: EC declaration of conformity provided in respect of lifting equipment to which the Lifting Operations and Lifting Equipment Regulations 1998 apply.

Retention period: For as long as the lifting equipment is being operated.

Examining lifting equipment

Record: Reports of thorough examination of lifting equipment, accessories, and written records of any defects discovered.

Retention period: Varies – until equipment ceases to be used or minimum two years after the report, whichever is later.

Risk assessments

Record: Significant findings of risk assessments; groups of employees at particular risk; preventive and protective measures.

Retention period: No time limit specified.

Classified persons, overexposure and ionising radiation

Record: Health records of classified persons and employees exposed to ionising radiation.

Retention period: Until the person has or would have attained the age of 75 years, but in any event for at least 50 years from the date of the last entry.

Exposure to lead

Record: Health record of an employee who is, or is liable to be, exposed to lead and under suitable medical surveillance.

Retention period: Minimum of 40 years from the date of the last entry.

Examinations of local exhaust ventilation and respiratory protective equipment

Record: Prescribed examinations and tests of local exhaust ventilation plant and respiratory protective equipment and of the repairs carried out.

Retention period: Minimum of five years from the date on which it was made.

Exposure to asbestos

Record: Health records and medical examination certificates relating to employees exposed to asbestos.

Retention period: Minimum of 40 years from the date of the last entry; minimum 4 years for medical certificates.

Exposure to specified hazardous substances

Record: Health surveillance records of persons exposed to substances hazardous to health.

Retention period: 40 years from the date of the last entry made in it.