

ALD Automotive Ltd Colleague & Contractor Data Protection Policy

Produced by
Louise Gaskill
Data Protection Officer

Contents

Version Control	3
Introduction.....	5
What this Policy Covers	5
Explanation of Terms Used in the Policy	5
Examples of “Personal Data” and “Special Category Personal Data”	5
Information & Data Security	7
Types of Personal Data Collected	8
Data Collected from Company Car Drivers / Ad-hoc Drivers.....	8
Accident Management	9
Breakdown / Tyres / Windscreens etc.	9
Occupational Road Risk & Licence Checking.....	10
Telematics Data.....	10
Parking / Speeding Fines etc.	11
Damage Recharges.....	11
How ALD collects your Personal Data.....	12
Examples of how ALD may collect your Personal Data	12
How ALD uses Personal Data	13
Disclosure of Personal Data by ALD	15
Recipients of Personal Data	15
Special Category Personal Data	17
Diversity Monitoring	17
Overseas Transfers	17
Monitoring & Recording of Communications.....	18
General	18

Electronic Communications	19
Data Scanning, SharePoint and Use of Company Systems	21
Inspection	21
Retention of Personal Data	22
Changes to Personal Details.....	22
Your Rights	23
The Right to be Informed	23
The Right of Access	23
The Right to Rectification	23
The Right to Erasure.....	23
The Right to Restrict Processing.....	23
The Right to Data Portability	24
The Right to Object	24
Queries Relating to Other SG Entities.....	24

Version Control

Date	Updated by	Modifications
February 2016	L Gaskill	New document created (version 1.0) based on SG London's Policy
June 2016	L Gaskill	Version 1.1 Amended section on Occupational Road Risk to reflect movement to Facilities Management
June 2017	L Gaskill	Version 1.2 Updated to reflect CCTV at new Oakwood Park site.
March 2018	L Gaskill / J Monk	Version 2.0 Updated to reflect new provisions under the GDPR • Change of the term "sensitive personal data" to "Special Categories" of data • Addition of details regarding the data scanning process • Data Retention Schedule added • Expanded section on Data Subject Rights
November 2018	L Gaskill	Version 2.1 Amended to remove references to Good email application and replace with Blackberry Work.
January 2019	L Gaskill	Version 2.2 Updated to reflect new Employee Car Benefit Scheme
May 2019	L Gaskill	Version 2.3 Annual Review including clarification of email inbox access, addition of new site CCTV locations and inclusion of Occupational Health provider
September 2019	L Gaskill	Version 2.4 Updates for use of app for telematics and screen / call recordings
November 2019	L Gaskill	Version 2.5 Updates to cover SMCR – regulatory references and retaining records relating to misconduct Sharing employee data with training providers in anticipation of using LinkedIn Learning
May 2020	L Gaskill	Version 2.6 Annual Review for Staff Deployment. Addition of information collected in relation to Covid-19 resource planning. Clarification of staff photos policy.

		Addition of Yammer to systems that are monitored and recorded. Addition of daily employee screening against sanctions lists
March 2021	L Gaskill	Version 2.7 Change of employee having to withdraw permission for photograph usage to ALD always asking permission in every instance. Addition of electric vehicle scheme details. Addition of expenses administrator as a recipient of employee data
March 2022	L Gaskill	Version 2.8 – Annual Review Addition of Diversity monitoring recording in PeopleSoft Addition of MS Teams in electronic communications Addition of Flex Benefits provider
March 2023	L Gaskill	Version 2.9 – Annual Review Updated to include Peoplesoft deletion period as this is now active Change of all references to “employees” to “colleagues” to reflect internal policy

Introduction

What this Policy Covers

ALD Automotive Ltd (“ALD” or “us”) gathers, stores and processes personal data in accordance with the Data Protection Act 2018 (“DPA”) and from 25th May 2018, the General Data Protection Regulation (GDPR). This Policy provides an overview of how ALD does this only in the context of your employment or engagement with ALD and is part of ALD's wider data protection policy.

This policy applies to all colleagues, contractors, agency staff and seconded staff.

This policy covers data that is held electronically and also applies to well-structured paper-based filing systems.

Explanation of Terms Used in the Policy

“Personal Data” is data which relate to a living individual who can be identified:

- (a) from those data, or
- (b) from those data and other information, which is in the possession of, or is likely to come into the possession of, the data controller (ALD),

and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

“Special Categories of Personal Data” (known as “Sensitive Personal Data” prior to GDPR) is personal data relating to your racial or ethnic origin, political opinions, religious or other similar beliefs, trade union membership, physical or mental health, sexual life or the commission or alleged commission of any offence, any proceedings for any offence committed or alleged to have been committed by you, the disposal of such proceedings or the sentence of any court in such proceedings.

Examples of “Personal Data” and “Special Category Personal Data”

Personal Data:

- Information held for payroll purposes – your salary, pension contributions, tax code and bank details;
- Performance review information held about you in the eValuation system and Learning Hub;
- An email you send to a colleague describing a different colleague's social behaviour could contain personal data about the sender, recipient and any person mentioned within it (the context of the email makes a difference).

Special Category Personal Data:

- Information you give to ALD about your racial or ethnic origin for diversity monitoring;
- A sickness certificate or report relating to you (whether it is scanned and held on ALD's computer systems or it is in a paper file behind a tab with your name on it, e.g. a dedicated HR file for storing that type of information).
- Information held by the business relating to any criminal or driving convictions you may have.

Information & Data Security

It is ALD's policy to protect your right to privacy. ALD will take all reasonable steps to ensure that adequate technical and operational security measures, confidentiality obligations and compliance procedures are in place to prevent inappropriate access to, and alteration or deletion of, personal data. ALD operates information security policies and guidelines relating to electronic data and information, which may include personal data.

By adhering to ALD's information security policies and guidelines, colleagues can themselves take appropriate steps to help to prevent unauthorised disclosure, alteration or use of their personal data. You are encouraged to refer to the Information Security policies and guidelines held on SharePoint.

Please also refer to the IT Security Policy section of the Employee Handbook which details fully ALD's E-mail & Internet Usage Policy.

Any misuse of ALD's information or electronic communication systems, including unauthorised access to or disclosure of personal data, may lead to instigation of disciplinary proceedings and disciplinary action being taken as a result. ALD may also consider commencing civil proceedings or reporting the matter to the Police.

Types of Personal Data Collected

In the course of your recruitment and employment, ALD may process personal data and Special Category personal data. This typically includes the following information relating to you:

- Personal details, including name, address, date of birth, age, marital status, family information (specifically dependent and partner information in relation to Covid-19 planning), emergency contacts;
- Education, qualifications, career history, skills and experience;
- Identification documentation, such as a photocopy of your passport, driving licence and / or ID card which may include a photograph of your face and shoulders;
- National insurance number, bank details, financial background, compensation, benefits, share scheme records, health and pension details;
- Performance records, appraisals, disciplinary and training records absence and time-keeping records, regulatory check information and records, unspent criminal records, family leave entitlements; and
- Details of your access to ALD premises (including CCTV images within and outside of buildings), systems, networks, software, websites and applications, including access, location and communications data. CCTV recording is present at the following locations at ALD offices –
 - Customer Excellence Centre: in the car park; on the car park barrier; on front and rear doors; and in the Comms room.
 - Innovation & Development Centre: the car park and front door
 - ALD SA Office, Northampton: front door and the car park (controlled by the Business Park)
 - Milton Keynes site: yard areas; car park and front door.
- Photographs and / or videos of colleagues may be taken during the course of their employment at ALD for internal and external marketing purposes. Your permission will always be sought to use these photographs and you can refuse.

Data Collected from Company Car Drivers / Ad-hoc Drivers

If you drive an ALD vehicle either as a company car driver or an ad-hoc driver, it is necessary for ALD to collect personal data in conjunction with your use of this vehicle and to share this data with certain third parties. All third parties carrying out services for ALD are subject to

comprehensive supplier agreements which contain provision for the protection of all personal data provided to them.

From April 2021, ALD are moving to all eligible colleagues being issued with their choice of fully electric, battery electric vehicle or plug-in hybrid vehicle. As part of this policy, colleagues can choose

There are two charging and fuel options available to eligible colleagues -

- Option 1 – the company pays for all electricity and the colleague repays their personal mileage to ALD
- Option 2 – the colleague pays for their own fuel, electricity and petrol (if applicable) and they are paid for any business journeys undertaken.

All vehicles will be fitted with a telematics device (see Telematics data below) and all mileage is programmed to private mileage.

In order to participate in Option 1 above, the colleague must have a company approved charger installed at their nominated location. The charger will be provided by ChargePoint and you will be sent details of how to sign up to their services. ChargePoint will provide you with their own Privacy Policy containing details of how they use your personal data.

ChargePoint will share cost data with ALD to enable the administration of this scheme. Access to this data will be restricted to relevant members of the HR & Finance teams.

Accident Management

If you have an accident whilst driving an ALD vehicle, this will be managed by ALD's nominated third party supplier for this service. This includes, but is not necessarily limited to –

- Details given at First Notification of Loss (FNOL), e.g. driver name, date of birth, address, details of the accident location, whether the journey was being undertaken for business or pleasure and any injuries sustained.
- Information collected at FNOL will be shared with the third party supplier's nominated repairers and ALD's insurer.
- A monthly report of all accidents involving ALD vehicles is produced for the purposes of management reporting.

Breakdown / Tyres / Windscreens etc.

If your vehicle is involved in a breakdown, personal information relating to you and your location will be taken by the third party supplier responsible for carrying out ALD's breakdown service. Similarly, if the vehicle requires a tyre or windscreen repair / replacement, your personal details will need to be provided to the supplier carrying out this service.

Occupational Road Risk & Licence Checking

All of ALD's services relating to Occupational Road Risk are carried out by one supplier. This includes licence checking, risk assessment and any required training interventions.

Occupational Road Risk assessments are carried out online for all required drivers. At the point of completing this, you sign up to the supplier's Data Protection mandate to give permission for your information to be used. The information provided includes special category data e.g. driving convictions and health conditions. This mandate includes your employee number and department, date of birth, name, address and driving licence details. At this point the third party supplier uses the information to run a DVLA check on the licence.

Reports are run from the system on a monthly basis by the Facilities department. This includes DPA Mandate Expiry, Company Car Driver Check, Licence Check / Status & Points (for ALD drivers and their nominated driver) and Under 25 drivers (provided to our insurance broker).

Ad-hoc drivers are required to complete the DPA mandate and licence checking process when the need arises for them to use an ALD company vehicle.

Telematics Data

In May 2019, ALD transferred all company car drivers to a new Car Benefit Scheme. All company car drivers will be part of this scheme with no exceptions.

All vehicles will be fitted with a telematics unit to assist with mileage capture. Information collected from the unit includes the following:

- Odometer readings and total mileage
- Date and time of any journey; the distance travelled and the duration of the journey
- Fuel consumption and fuel events
- Vehicle condition data, including but not limited to, service alerts, fault codes and battery levels
- Crash data
- GPS co-ordinates during a journey
- Behavioural data, including but not limited to, revving, idling, braking, accelerating, speeding, swerving and cornering
- GPS co-ordinates at the start and end destination of a journey
- Postcodes for the start and end of a journey

The journey data is sent directly to the telematics service providers for storage and processing. By choosing to use a company car, journey data will automatically be captured about the use of your car.

All journeys will be automatically marked as personal until you use the portal to identify them as a business journey.

In due course, all company car drivers will be asked to download a smartphone app to record their journey information and the web portal will no longer be in use.

Parking / Speeding Fines etc.

If the vehicle you are driving is issued with a speeding / parking / bus lane fine etc. whilst you are driving, ALD are obliged to provide the driver details when responding to the issuing authority. You will always be notified of any fines issued against yourself in a letter from the Fleet Support department. If the fine will result in points added to your licence, a copy of this letter will also be sent to the HR department.

Damage Recharges

In order for ALD to be able to make the necessary recharges for damage on company cars, an account will be set up to facilitate this process in the Accounts module of Fleetware. This account will contain each staff member's name, address and date of birth.

How ALD collects your Personal Data

ALD collects your personal data primarily from:

- the information you submit during the course of your employment or engagement with ALD; and
- through monitoring and recording communications and/or use of technology, as is explained further in this policy.

Examples of how ALD may collect your Personal Data

- Where you provide information to ALD about yourself or your family, e.g. in application forms and through information provided during the recruitment process, including background and reference checks; health questionnaires for insurance benefits and family information to assist with Covid-19 resource planning;
- Where information about you or your family is provided to ALD by a **third party**, e.g. a medical adviser or a person giving a reference about you;
- Where information is created as a result of generally administering your ongoing employment, e.g. payroll processes, benefit and pension scheme operation, sickness absence, performance assessments and career management processes.

How ALD uses Personal Data

ALD may use your personal data before, during and after employment, for all purposes connected with your employment or engagement, including but not limited to:

- Pre-employment checks;
- Once employed, daily screening checks against sanctions lists to check for any flags that would be of concern;
- Equal opportunities and diversity monitoring;
- Employment administration, e.g. career management and appraisals, education and training, disciplinary activity, remuneration administration and reviews;
- Operation and management of IT, telephone and other electronic communications systems;
- Assessment of compliance with ALD / SG policies and procedures;
- To comply with regulatory obligations and carry out HR and compliance functions;
- To ensure our Insurance Broker and our Insurer can define the risk levels for the drivers using vehicles on ALD insurance, both colleague and nominated drivers;
- Payroll and remuneration administration and management, e.g. salary payments, provision of flexible benefits and other colleague benefits, operation of bonus and incentive schemes, pension schemes and calculating tax payable on earnings and benefits;
- To comply with any legal and regulatory obligations and requests anywhere in the world, including reporting to and/or being audited by national and international regulatory, enforcement or exchange bodies;
- Where disclosure is required by or ALD wishes to co-operate in an investigation by a competent authority anywhere in the world, e.g. a Court or Tribunal, a regulatory authority or governmental body or department;
- Where disclosure is required or is deemed appropriate as part of legal proceedings or to exercise and/or defend ALD's legal rights;
- Carrying out legal and company secretarial activities;
- Where disclosure relates to a Corporate Social Responsibility (CSR) or another social event in which you are participating that ALD is involved in organising;
- When we need to store and use your personal contact details (e.g. mobile phone numbers and email addresses) for the purposes of maintaining the Business Continuity programme

and in the event that we need to invoke this process and communicate with you outside of normal office hours; and

- Otherwise in connection with your employment; in the course of ALD's legitimate business; or as required or permitted by law.

Disclosure of Personal Data by ALD

Recipients of Personal Data

A list of the main third parties that the ALD HR department discloses personal data to in the general course of its business (and the purpose of doing so) is maintained by ALD. If you require further information, please contact the HR Department.

ALD may disclose personal data to other Société Générale Group companies and to third parties for the uses described in the section “How ALD uses Personal Data”. In particular, information containing personal data may be disclosed to:

- ALD's accountants and professional advisers;
- ALD's Insurance Broker;
- ALD's insurers in relation to accidents and / or damage to a business vehicle;
- ALD's payroll, pension scheme administrators and other third party entities involved in the administration of colleague remuneration and benefits;
- ALD's Occupational Health provider if a referral is requested by the colleague or the HR department;
- Service providers and other organisations that carry out processing operations on ALD's behalf, including our chosen colleague expenses administrator;
- Service providers that carry out the processing of benefits on ALD's behalf, including our chosen Flex Benefits System provider;
- Exchanges and clearing houses;
- Colleague benefits advisors;
- Third parties to whom ALD is required to transfer data by law or regulatory requirement (such as HMRC, the PRA, FCA and Governmental bodies);
- Those third parties to whom the disclosure is warranted to protect against fraud or other illegal activities (e.g. disclosure to the FCA) or to enable ALD to carry out its legitimate business activities;
- Regulatory bodies or external agencies for the purpose of investigations or enquiries in relation to which ALD is co-operating;
- Third parties in connection with legal proceedings (including prospective legal proceedings);

- Third parties involved in organising events on ALD's behalf (including CSR events); and other members of the Société Générale Group;
- The police, as if a business vehicle has been stolen, we will disclose telematics data to assist in the recovery of the vehicle. This may contain personal data relating to the user of the vehicle;
- The Vehicle and Operator Services Agency (VOSA), if a business vehicle you have been using is involved in a road traffic collision resulting in a fatality.
- A requestor asking for details in order to fulfil a regulatory reference, in line with the Senior Managers & Certification Regime which came into effect in December 2019. References can be applied for whilst you are still in ALD's employment and for up to six years after the termination of your employment with ALD.
- Training companies and apprenticeship providers in order to provide you with external training services

ALD will not sell or transfer your personal data to any third party for that party to use for direct marketing purposes without your prior consent.

Special Category Personal Data

Data processing may include the processing of special category personal data about you. The most common processing of special category personal data by ALD occurs where:

- Information about your race, sex, health or religion/belief is processed in connection with equal opportunities activities;
- Information about your health and sickness is used to operate health-related insurance or benefit schemes, for sickness absence administration and management, to manage a referral to our occupational health provider (when applicable) and to comply with ALD's duties regarding the health and safety of its workers;
- Your criminal record is obtained and reviewed in connection with pre-employment checks and regulatory compliance;
- You have given your consent (for example, in relation to your participation in a CSR event);
or
- It is otherwise required or permitted to do so by applicable law.

Diversity Monitoring

In February 2022, a “Diversity Profile” section was added to PeopleSoft. This allows ALD to obtain an accurate picture of the current diversity and inclusion position. The data includes gender identity, ethnicity, sexual orientation, religion, disability and caring responsibilities. Creating your diversity profile is entirely optional, but in doing so will help ALD to shape a diversity and inclusion strategy. All data is anonymised for reporting purposes. Access to the source data is restricted to the HR diversity data owner only.

Overseas Transfers

Processing will include transferring personal data to recipients located in France and also other countries where the Société Générale Group has business operations, such as Asia, or provides services (including countries outside the European Economic Area (EEA) such as Société Générale’s offshore service centres in India and other countries. Transfers will include (but not be limited to) special category personal data which is essential for the administration of your employment and the operation of ALD's and/or the Société Générale Group's business. If we transfer your information outside the EEA in this way, we will take steps to ensure that your privacy rights continue to be protected in accordance with applicable laws and regulations and ALD’s policies and standards.

Monitoring & Recording of Communications

General

In most cases, it will be obvious when personal data about you is collected. For example, if you want to participate in a health-based insurance scheme it is likely that you will complete a form and give information about you or your family and return it to ALD. In this case it is obvious to you what kind of personal data is collected and the reason why. There is no legal definition of monitoring but, generally speaking, gathering information from sources in a systematic way is more commonly called monitoring and can arise in less obvious ways, such as information gathered through security measures, e.g. security pass entry/exit data.

ALD may monitor, record and inspect the following sources of information where it is in its legitimate business interests to do so; to check for compliance with ALD's policies; to comply with applicable law and regulations; to facilitate administration and support; to assist with security, crime prevention and fraud purposes; to investigate or detect unauthorised use of ALD services, systems or other materials; or where it is necessary and proportionate, to the extent permitted by law:

- Electronic communications (emails, instant messages, voicemails, telephone calls, text messages, fax transmissions, Internet use, Intranet use, Yammer and Webex / Webex Teams, MS Teams);
- Remote access capabilities (for example, VPN and);
- CCTV recordings;
- Records of printing and photocopying;
- Security pass data;
- Other communications (such as letters/envelopes or packages); and
- Using monitoring devices or other technical or physical means by authorised ALD personnel.

Data obtained from monitoring may also be analysed and:

- used as evidence in any disciplinary or other proceedings against its personnel brought by ALD or an external authority (such as the FCA, the Police, or other regulatory authorities or agencies) or a related investigation; and
- provided to regulatory bodies or agencies having jurisdiction over any of the SG Group of Companies in relation to investigations or enquiries.

Whilst moderate non-business use of the Internet, email and telephones is permitted in accordance with applicable ALD policies and guidelines, all activity is logged, recorded and monitored because it is not possible to differentiate between business and non-business calls and ALD may use activity logs to review compliance with such policies and guidelines.

Electronic Communications

Electronic communications (e.g. telephone calls, fax transmissions, emails, instant messaging, text messaging and Internet access) may be monitored and recorded in accordance with applicable laws for the following permitted business-related purposes:

- Colleague supervision and disciplinary purposes;
- Establishing the existence of facts (e.g. recording evidence of business transactions);
- Ascertaining compliance with regulatory or self-regulatory practices or procedures which relate to ALD's business;
- Ascertaining or demonstrating standards which are achieved or ought to be achieved by persons using ALD's systems;
- Preventing or detecting crime;
- Investigating or detecting unauthorised use of ALD's telecommunications systems and other materials (e.g. monitoring to ensure compliance with ALD's policies and procedures and to evaluate the quality of customer service);
- Ensuring the effective operation and security of ALD's information and telecommunications systems (e.g. automated virus checking and backing up).

Fixed line telephone calls are recorded in all areas of ALD's business that are subject to regulatory supervision (i.e. those which deal with consumers) as well as other selected individuals within the organisation. All such calls are recorded because it is not possible to differentiate between business and non-business calls, therefore you must assume any call you make or receive in a regulated area is being recorded. ALD has the right to record any calls within any area of the business for training and quality purposes and consequently all staff should assume their calls could be recorded at any time. If you would like confirmation if calls on your phone extension are recorded, this can be checked at any time with either your manager or the IT Infrastructure team. In order to comply with FCA regulations, recordings of phone calls are retained for three years.

All telephone activity is logged (whether on a recorded line or not). This log includes extension number, time, date, contact number and the cost of the call. Monthly reports may be generated to review usage and may be used as a basis for disciplinary action or a related investigation.

From 1st October 2019, ALD will have the ability to record the screen content of the telephone system. This will be used for system training purposes only. The intention is to retain these

recordings for three months, however, some specific recordings may be retained for longer if deemed necessary. Please speak to your Team Leader or Line Manager if you would like confirmation that this applies to your usage.

Please note that it is not possible for individuals to turn off the screen or call recording functions, so you should assume that everything is recorded.

All calls made and SMS messages sent on ALD mobile telephones are logged but are not recorded. A monthly bill is generated and provided to the IT Director for authorisation. This contains the number, time, date and cost of the call.

Use of Email and the Internet is monitored as explained in ALD's Email and Internet Usage Guidelines, but you should note that:

- All Internet activity is logged. These logs indicate the page accessed and the time and date of access for each internet user account. These logs can be accessed at any time by authorised personnel for any of the above purposes;
- All internal and external email traffic is logged. This log contains details of the sender, recipient and time of transmission, which are automatically recorded without differentiation between personal and business-related emails. ALD also retains the content of transmitted emails via its automated backup processes. This information may be accessed by authorised personnel at any time for any of the above purposes. Emails are not opened or read as a matter of routine;
- Use of most instant messaging services is prohibited in accordance with ALD's social media policy. The only approved instant messaging services are Jabber (part of the Cisco phone system), Lync / Skype for business (part of Office 365) and Webex. Jabber does not currently log conversations. Skype for business records logs of all conversations outside of Outlook.

Data Scanning, SharePoint and Use of Company Systems

As part of the company-wide project to ensure compliance with the GDPR, ALD has used a piece of software called DatAdvantage to discover information about the data held in our environments. It has scanned all data stored on our SharePoint and Windows to servers to accurately identify all locations where personal data has been stored.

Anything stored on a company device is deemed company information and has therefore been scanned and analysed by this system. If you have stored personal files in your OneDrive location on SharePoint, these will have been scanned as part of this process.

IT administrators who have been granted privileged access to the corporate network, have been given this access in order to carry out the requirements of their role and they are bound by a duty of confidentiality. All computer and associated equipment remain at all times the property of the company. The company will maintain and perform operations necessary to safeguard the assets of the business and the information contained therein. There should be no expectation of privacy in your use of any company systems in the monitoring that may be necessary for this purpose, or for the purpose of evaluating the work performance of any individual. Such monitoring may extend to email, internet, files, or any other electronic storage or communication.

Inspection

Unopened and / or unread electronic and paper communications may be checked and read by authorised ALD personnel to ensure that ALD can deal with any business-related matters (e.g. in an individual's absence) or for another permitted purpose (see above). Communications marked as "private" or "personal" will not be opened unless it is necessary to do so in order to decide if that communication is business-related or not. Authorised ALD personnel may access electronic communications or a physical area, such as a desk or cupboard, for these purposes.

In the event of both planned and unplanned absence, your email account may be accessed by your Line Manager in order to maintain the consistent running of the department. This means that any previously sent or received messages can be accessed, as well as any unread items in your inbox. All occurrences of granting this type of access are documented with the reasons this is required and signed off by the relevant HR Business Partner.

Retention of Personal Data

ALD retains personal data for as long as necessary to fulfil the purpose for which it was collected or to comply with legal, regulatory or internal policy requirements. During 2018, there was an extensive exercise to transfer all paper files to electronic format. Documents older than 7 years have not been part of this exercise and all paper files have now been destroyed.

Retention periods relating to specific HR records are as follows:

DATA	RETENTION PERIOD	DELETION METHOD
Applicant Data & Equal Opportunities data	12 months	Obfuscation 12 months after the recruitment decision
Payroll Files	7 years from the date of creation	Deletion at the end of each month
Personnel Files – Leavers	7 years from end of employment Information relating to serious misconduct for SMCR Senior Managers and Certified Persons will need to be retained indefinitely in order to comply with the Regime.	Paper records held at external facility are automatically shredded at the 7-year mark
Personnel Files – Current Colleagues	Electronic files are kept for the duration of employment Disciplinary / grievance documentation is removed 12 months after the event.	Notification received once 12 months has passed and documents deleted
Peoplesoft	10 years	Deletion

ALD's Document and Record Control Policy details how long information is kept on systems not related to HR records. Please consult this Policy if you require any further information.

Changes to Personal Details

In order that ALD can meet its legal obligations, you are required to make sure that ALD has an accurate record of your personal details. Any changes must be submitted to the HR department as soon as is reasonably possible (e.g. changes of home address or emergency contact). Please remember to keep this important information up to date.

Your Rights

Under the General Data Protection Regulation, data subjects i.e. ALD colleagues, have enhanced rights to the handling and processing of their personal data. These are as follows:

The Right to be Informed

- As a data subject, you have the right to be informed about all the ways in which ALD uses your personal data, who it is shared with, where it is stored and for how long.
- The way we have chosen to do this is through this document (the ALD Colleague Data Protection Policy). Your acceptance of this policy will be recorded through the Learning Hub.
- We will review and update this Policy at least annually and you will be given the chance to review and accept any changes that have been made.

The Right of Access

- As a data subject, you have the right to see a copy of all the personal data that we hold about you.
- Under the GDPR, we must provide this to you within one month and we must no longer charge a fee for doing this.

The Right to Rectification

- You are entitled to have any inaccurate personal data held about you corrected in a timely manner.
- Under GDPR, ALD have one month to correct anything that is requested, but we would always endeavour to make any requested changes as soon as possible.
- Please ensure that any changes to your personal details are submitted to HR as soon as possible so that your records can be kept up to date.

The Right to Erasure

- You can request that data held about you is removed from our records, also known as the “right to be forgotten”.
- However, this is not an absolute right and ALD will have to consider whether any requests are able to be actioned given our legal obligations to maintain accurate records and information.

The Right to Restrict Processing

- You can request that ALD restrict or suppress your personal data.
- However, as with the right to erasure, this is not an absolute right and we would need to consider whether any request could be actioned.

The Right to Data Portability

- As a data subject, you have the right to request a copy of your personal data to use for the purpose of providing it to another organisation.
- ALD will need to respond to such a request with the information in a usable format.

The Right to Object

- Individuals have a right to object to the processing of their personal data.
- However, it is likely that any such objections can be refused due to the necessity of ALD having to process the data in order to carry out the contract of employment between themselves and a data subject.
- As with all other rights, any objections will always be considered and responded to accordingly.

If you wish to exercise any of these rights, you should contact ALD's Data Protection Officer at dpo@aldautomotive.com, copying in UK-HR.

Queries Relating to Other SG Entities

If you have a query regarding the processing of your personal data by any other ALD or SG Group company please contact your usual HR representative, explaining which company your query relates to and that your query relates to data protection.



Mobility is changing.

Autonomous vehicles and connected travel might seem a little way off, but the future is just around the corner and, with technology making the world smaller, we are committed to helping you explore it. From corporate fleets to individual ownership and shared usage we are helping 1.6 million people worldwide embrace a new way to travel. We are here to make your journey as exciting as your destination.

BRISTOL (HEAD OFFICE)

Oakwood Drive, Emersons Green, Bristol
BS16 7LB
TEL: 0117 908 2000

BRISTOL (INNOVATION AND DEVELOPMENT CENTRE)

1 Harlequin Business Park, Fieldfare, Emersons Green, Bristol
BS16 7FN
TEL: 03700 011 181

MILTON KEYNES

66 Denbigh Road, Bletchley, Milton Keynes,
MK1 1DF
TEL: 01908 272 290

ukinfo@aldautomotive.com, www.aldautomotive.co.uk

ALD Automotive Limited - Oakwood Drive - Emersons Green - Bristol - BS16 7LB - United Kingdom
Tel: +44 (0)117 908 2000 - Fax: (0) 117 908 9000 - www.aldautomotive.co.uk - www.socgen.com
Co. Reg. No. 987418 England - Reg. Office: Oakwood Drive - Emersons Green - Bristol BS16 7LB UK

ALD Automotive Limited is incorporated in the UK and authorised and regulated by the Financial Conduct Authority.
We may monitor or record any communication between you and ALD Automotive for quality control and training purposes.



ALD Automotive Ltd Colleague & Contractor Data Protection Policy

Produced by
Louise Gaskill
Data Protection Officer